*Supplemento ordinario alla "Gazzetta Ufficiale,, n. 272 del 19 novembre 2004 - Serie generale*

*Spediz. abb. post. 45% - art. 2, comma 20/b*
*Legge 23-12-1996, n. 662 - Filiale di Roma*

**DELLA REPUBBLICA ITALIANA**

*PARTE PRIMA* **Roma - Venerdì, 19 novembre 2004** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06 85081



**N. 167**

# MINISTERO DELLA GIUSTIZIA

DECRETO 14 ottobre 2004.

# Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile.

# S O M M A R I O

## MINISTERO DELLA GIUSTIZIA

# DECRETI, DELIBERE E ORDINANZE MINISTERIALI

## MINISTERO DELLA GIUSTIZIA

DECRETO 14 ottobre 2004.

**Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile.**

IL MINISTRO DELLA GIUSTIZIA

Visto il decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

Visto il decreto del Presidente della Repubblica 13 febbraio 2001, n. 123;

Visto il decreto ministeriale 27 marzo 2000, n. 264;

Visto il decreto ministeriale 24 maggio 2001;

Vista la delibera del Centro nazionale per l'informatica nella pubblica amministrazione del 19 febbraio 2004, n. 11;

Sentito il Centro nazionale per l'informatica nella pubblica amministrazione, con il parere del 22 settembre 2004, dal quale parzialmente ci si discosta, ove si ravvisa la superfluità del certificato per la crittografia delle informazioni trasmesse, ritenendo opportuno garantire la massima sicurezza nei raccordi comunicativi, in particolare, nel punto d'accesso e nel gestore centrale; ritenuta, inoltre, l'opportunità di limitare l'utilizzazione delle caselle di posta elettronica alle sole comunicazioni del processo telematico, in considerazione dell'inesperienza degli utenti, in fase di prima attuazione;

Sentito il Garante per la protezione dei dati personali, con il parere del 23 luglio 2004, dal quale parzialmente ci si discosta, ove si ravvisa l'utilità di inserire ulteriori richiami, sostanziali e formali, al decreto legislativo n. 196 del 2003, trovando tale normativa, di rango superiore, comunque applicazione; ritenuta, inoltre, la non necessità di individuare i titolari del trattamento dei dati personali, esulando la problematica dal ristretto ambito delle regole tecniche; ritenuta la non opportunità di cumulare, necessariamente, il responsabile della sicurezza con il responsabile del trattamento dei dati personali, attese le diverse finalità che possono richiedere professionalità differenti ed, infine, di mantenere le ampie condizioni di accesso agli avvocati dello Stato, in ragione della loro rappresentanza, fissata dall'art. 1 del regio decreto 30 ottobre 1933, n. 1611;

Decreta:

*Capo I*

PRINCIPI GENERALI

Art. 1.

*Ambito di applicazione*

1. Il presente decreto stabilisce le regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile di cui all'art. 3, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123.

Art. 2.

*Definizioni*

1. Ai fini del presente decreto si intendono per:

*a)* SICI: sistema informatico civile come definito nel decreto del Presidente della Repubblica 13 febbraio 2001, n. 123;

*b)* gestore centrale: struttura tecnico-organizzativa che, nell'ambito del dominio giustizia, come definito all'art. 1, comma 1, lettera *e)* del decreto ministeriale 13 febbraio 2001, n. 123, fornisce i servizi di accesso al SICI ed i servizi di trasmissione telematica dei documenti informatici processuali fra il SICI ed i soggetti abilitati, secondo le norme riportate nel presente decreto;

*c)* gestore locale: sistema informatico che fornisce i servizi di accesso al singolo ufficio giudiziario o all'ufficio notifiche esecuzioni e protesti (UNEP), ed i servizi di trasmissione telematica dei documenti informatici processuali fra il gestore centrale ed il singolo ufficio giudiziario o UNEP;

*d)* certificazione del difensore: attestazione al difensore di iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati ovvero di possesso della qualifica che legittima l'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva;

*e)* punto di accesso: struttura tecnico-organizzativa che fornisce ai soggetti abilitati, esterni al SICI, i servizi di connessione al gestore centrale e di trasmissione telematica dei documenti informatici relativi al processo, nonché la casella di posta elettronica certificata, secondo le regole tecnico-operative riportate nel presente decreto;

*f)* autenticazione: operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, contenente un certificato di autenticazione, secondo la previsione dell'art. 62;

*g)* firma digitale: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al decreto legislativo 23 gennaio 2002, n. 10;

*h)* fascicolo informatico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, ovvero le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo;

*i)* soggetti abilitati: tutti i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:

1.1. soggetti abilitati esterni privati: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;

1.2. soggetti abilitati esterni pubblici: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali;

1.3. soggetti abilitati esterni: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;

1.4. soggetti abilitati interni: i magistrati, il personale degli uffici giudiziari e degli UNEP;

*j)* casella di posta elettronica certificata per il processo telematico (CPECPT): indirizzo elettronico, per il processo telematico, dei soggetti abilitati.

Art. 3.

*Gestore centrale*

1. Il gestore centrale è il punto unico di interazione, a livello nazionale, tra il SICI ed i soggetti abilitati esterni.

2. Il gestore centrale è attivo presso il Ministero della giustizia.

Art. 4.

*Gestore locale*

1. Il gestore locale è parte del sistema informatico dell'ufficio giudiziario e dell'UNEP, come definito nel decreto ministeriale del 24 maggio 2001, e rispetta i requisiti tecnici ed organizzativi definiti in tale ambito.

2. I gestori locali sono attivi presso gli uffici giudiziari e gli UNEP.

Art. 5.

*Sistemi informatici di gestione della cancelleria e dell'UNEP*

1. Il sistema informatico di gestione delle cancellerie civili è costituito dall'infrastruttura hardware e software di gestione dei registri e dei fascicoli informatici.

2. Il sistema informatico di gestione degli UNEP è costituito dall'infrastruttura hardware e software per la gestione delle notifiche.

Art. 6.

*Punto di accesso*

1. I soggetti abilitati esterni accedono al SICI tramite un punto di accesso, che può essere attivato esclusivamente dai soggetti pubblici, di cui al comma 5, e dai soggetti privati, di cui al comma 6. Ciascun soggetto può avvalersi di un solo punto di accesso.

2. I punti di accesso forniscono un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema ed a non comprometterne i livelli di servizio, nel rispetto dei requisiti tecnici di cui all'art. 30.

3. La violazione, da parte di un punto di accesso, dei livelli di sicurezza e di servizio, comporta la sospensione ad erogare i servizi fino al ripristino di tali livelli.

4. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.

5. I soggetti pubblici, che possono attivare e gestire uno o più punti di accesso, sono:

*a)* i consigli dell'ordine degli avvocati, ciascuno limitatamente ai propri iscritti;

*b)* il Consiglio nazionale forense, limitatamente ai propri iscritti e agli iscritti dei consigli dell'ordine degli avvocati;

*c)* il Consiglio nazionale del notariato, limitatamente ai propri iscritti;

*d)* l'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;

*e)* il Ministero della giustizia, per i soggetti abilitati interni e in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui ai punti *a)* e *b)*;

*f)* il Ministero della giustizia, in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui al comma 6, al solo fine di garantire l'accesso agli esperti e ausiliari del giudice.

6. I soggetti privati, che attivano e gestiscono un punto di accesso, hanno i seguenti requisiti:

*a)* forma di società per azioni;

*b)* capitale sociale e requisiti di onorabilità di cui al decreto legislativo 1° settembre 1993, n. 385, art. 25, comma 1.

Art. 7.

*Certificazione dei difensori*

1. La certificazione del difensore è svolta dal punto di accesso, qualora questo sia gestito da un Consiglio dell'ordine degli avvocati o dal Consiglio nazionale forense, oppure dal gestore centrale sulla base di copia dell'albo fornita al Ministero della giustizia e dai consigli dell'ordine degli avvocati e dal Consiglio nazionale forense.

2. L'aggiornamento della copia dell'albo avviene entro 72 ore dalla comunicazione, dei provvedimenti di pertinenza, all'interessato.

3. Il Consiglio nazionale forense compie il servizio di certificazione dei difensori per i propri iscritti o, per gli iscritti dei consigli dell'ordine, su delega di questi ultimi.

Art. 8.

*Accesso dei soggetti abilitati esterni privati*

1. Per il difensore delle parti è necessaria, ai fini dell'accesso al SICI, l'autenticazione presso il punto di accesso di cui al capo quarto e la certificazione di cui all'art. 7.

2. Il SICI consente al difensore l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito e permette, negli altri casi, l'acquisizione delle informazioni necessarie per la costituzione in giudizio.

3. In caso di delega, rilasciata ai sensi dell'art. 9, regio decreto legislativo 27 novembre 1933, n. 1578, il SICI consente all'avvocato delegato l'accesso alle informazioni contenute nei fascicoli dei procedimenti patrocinati dall'avvocato delegante, previa comunicazione, a cura di parte, di copia della delega stessa al responsabile dell'ufficio giudiziario, che provvede ai conseguenti adempimenti. L'accesso è consentito fino alla comunicazione della revoca della delega.

4. La delega, sottoscritta con firma digitale, è rilasciata in conformità al modello previsto dall'art. 56.

5. Gli esperti e gli ausiliari del giudice accedono al SICI nel limite dell'incarico ricevuto e della autorizzazione, concessa dal giudice, alla consultazione e alla copia degli atti.

6. A seguito dell'autenticazione, viene trasmesso al gestore centrale il codice fiscale del soggetto abilitato esterno privato.

Art. 9.

*Accesso dei soggetti abilitati esterni pubblici*

1. Il punto di accesso autentica il soggetto abilitato esterno pubblico e trasmette il relativo codice fiscale al gestore centrale.

2. I dati, di cui al comma 1, sono utilizzati per individuare i privilegi di accesso alle informazioni contenute nel SICI.

3. Il SICI consente agli avvocati e procuratori dello Stato l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è parte una pubblica amministrazione.

Art. 10.

*Accesso dei soggetti abilitati interni*

1. I soggetti abilitati interni accedono al SICI attraverso la rete unica della giustizia (RUG) e attraverso il punto di accesso del Ministero della giustizia.

*Capo II*

GESTIONE DELLA POSTA ELETTRONICA

Art. 11.

*Casella di posta elettronica certificata del processo telematico*

1. I soggetti abilitati esterni, per utilizzare i servizi di trasmissione telematica dei documenti informatici, dispongono di un indirizzo elettronico e della relativa casella di posta elettronica, CPECPT, forniti e gestiti dal punto di accesso, nel rispetto dei requisiti di cui all'art. 12.

2. Ogni indirizzo elettronico, come definito nel decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, corrisponde ad una CPECPT.

3. Ad ogni soggetto, che interagisce per via telematica con il SICI, corrisponde un solo indirizzo elettronico.

4. Ogni CPECPT è abilitata a ricevere messaggi provenienti unicamente da altri punti di accesso e dal gestore centrale.

Art. 12.

*Requisiti del servizio di gestione della CPECPT*

1. La CPECPT garantisce la ricezione dei messaggi e la loro disponibilità per trenta giorni, successivamente il messaggio è archiviato e sostituito da un avviso contenente i seguenti dati: identificativo univoco del messaggio, mittente, data, ora e minuti di arrivo.

2. Il servizio di posta elettronica certificata restituisce al mittente una ricevuta breve di avvenuta consegna per ogni documento informatico reso disponibile al destinatario, cui è associata l'attestazione temporale di cui all'art. 45.

3. Salvo quanto previsto nel presente decreto e nell'allegato B, la posta certificata del processo telematico si conforma alle linee guida stabilite dal Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA).

4. L'avviso di cui al comma 1 è conservato, presso il punto d'accesso, per un periodo non inferiore a cinque anni.

Art. 13.

*Registro generale degli indirizzi elettronici*

1. Il registro generale degli indirizzi elettronici, attivo presso il gestore centrale, contiene l'elenco di tutti gli indirizzi elettronici attivati dai punti di accesso.

2. Il registro generale degli indirizzi elettronici è accessibile a tutti i soggetti abilitati, secondo le modalità previste dall'art. 19.

3. All'indirizzo elettronico delle persone fisiche, sono associate le seguenti informazioni:

*a)* nome e cognome;

*b)* luogo e data di nascita;

*c)* codice fiscale;

*d)* data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;

*e)* residenza;

*f)* domicilio;

*g)* stato dell'indirizzo: attivo, non attivo;

*h)* certificato digitale relativo alla chiave pubblica, da utilizzare per la cifratura;

*i)* consiglio dell'ordine o ente di appartenenza;

*j)* stato del difensore: attivo, non attivo.

4. All'indirizzo elettronico degli enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, sono associate le seguenti informazioni:

*a)* denominazione sociale;

*b)* codice fiscale;

*c)* data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;

*d)* sede legale;

*e)* certificato digitale relativo alla chiave pubblica da utilizzare per la cifratura;

*f)* stato dell'indirizzo: attivo, non attivo.

### Art. 14.

*Registrazione dei soggetti abilitati esterni al SICI*

1. L'accesso al SICI e la casella di posta elettronica si ottengono previa registrazione presso un punto di accesso.

2. La registrazione si ottiene con richiesta scritta, che il punto d'accesso conserva per almeno dieci anni.

3. Con la registrazione, il punto di accesso acquisisce i dati di cui all'art. 13, commi 3 e 4, e verifica l'identità del richiedente ed il relativo codice fiscale.

4. I difensori delle parti presentano, all'atto della registrazione, un certificato, rilasciato in data non anteriore a venti giorni, in cui il consiglio dell'ordine di appartenenza attesta l'iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati, oppure la qualifica che legittima all'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva.

5. Gli esperti e gli ausiliari del giudice presentano, all'atto della registrazione, il certificato della iscrizione all'albo dei consulenti tecnici o copia della nomina da parte del giudice dalla quale risulta che l'incarico non è esaurito.

6. Al momento della registrazione, i soggetti abilitati esterni comunicano al punto di accesso le seguenti informazioni:

*a)* nome e cognome;

*b)* luogo e data di nascita;

*c)* codice fiscale

*d)* residenza;

*e)* domicilio;

*f)* certificato digitale, relativo alla chiave pubblica, per la cifratura;

*g)* consiglio dell'ordine di appartenenza.

I soggetti abilitati esterni comunicano al punto di accesso ogni variazione delle informazioni di cui alle lettere *d), e), f)* e *g)*.

7. Le informazioni di cui al comma 6, unitamente alla qualità di difensore delle parti, di esperto o ausiliario del giudice, ed all'indirizzo elettronico assegnato e ad eventuali variazioni del suo stato, sono trasmesse dal punto di accesso al gestore centrale e, per i difensori delle parti, al consiglio dell'ordine di appartenenza.

### Art. 15.

*Obbligo di informazione*

1. I punti di accesso informano i titolari di indirizzi elettronici degli obblighi assunti in relazione al servizio offerto.

### Art. 16.

*Registro degli indirizzi elettronici del punto di accesso*

1. Il punto di accesso attiva un registro degli indirizzi elettronici che contiene l'elenco di tutti gli indirizzi elettronici emessi, revocati o sospesi dal punto di accesso.

2. Ad ogni indirizzo elettronico di persona fisica sono associate le informazioni di cui all'art. 13, comma 3.

3. L'indirizzo elettronico di enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, associa le informazioni di cui all'art. 13, comma 4.

4. Il difensore comunica al consiglio dell'ordine di appartenenza il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso, unitamente al proprio codice fiscale e ai dati identificativi del punto di accesso.

5. Il difensore delle parti, l'esperto o l'ausiliario del giudice comunica alla cancelleria competente il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso.

6. Il registro degli indirizzi elettronici è accessibile a tutti i soggetti abilitati, secondo le modalità previste dall'art. 19.

7. Per i soggetti abilitati esterni pubblici, ciascun punto di accesso comunica al Ministero della giustizia, per via telematica, tutte le informazioni di cui all'art. 13, commi 3 e 4, ed ogni loro variazione, al fine dell'inserimento nel registro generale degli indirizzi elettronici.

### Art. 17.

*Comunicazioni dei consigli dell'ordine degli avvocati e del Consiglio nazionale forense*

1. Al fine dell'inserimento nei registri degli indirizzi elettronici, i consigli dell'ordine degli avvocati e il Consiglio nazionale forense comunicano al Ministero della giustizia ed ai punti di accesso di riferimento, le seguenti informazioni e le loro variazioni, per via telematica, relative ai difensori:

*a)* nome e cognome;

*b)* luogo e data di nascita;

*c)* codice fiscale;

*d)* domicilio;

*e)* indirizzo elettronico, dichiarato e fornito dal punto di accesso;

*f)* data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;

*g)* stato dell'indirizzo: attivo, sospeso, non attivo;

*h)* dati identificativi del punto di accesso che fornisce il servizio di posta elettronica;

*i)* stato del difensore: attivo, sospeso, cancellato, radiato; con indicazione di inizio efficacia del provvedimento e di fine efficacia nell'ipotesi di provvedimento temporaneo.

2. La comunicazione di cui al comma 1 è sottoscritta, con firma digitale, dal presidente del consiglio dell'ordine ovvero del Consiglio nazionale forense, o da un loro delegato.

3. La comunicazione di cui al comma 1 è strutturata in linguaggio XML, secondo il formato definito nel decreto ministeriale di cui all'art. 52.

Art. 18.

*Requisiti tecnici dei registri degli indirizzi elettronici*

1. Il gestore centrale ed i punti di accesso rendono disponibile una copia operativa dei propri registri degli indirizzi elettronici e mantengono l'originale inaccessibile dall'esterno.

2. Il gestore centrale ed i punti di accesso garantiscono la conformità tra la copia operativa e l'originale dei propri registri e risolvono tempestivamente qualsiasi difformità, registrandola in un apposito giornale di controllo.

3. Le operazioni che modificano il contenuto dei registri sono consentite unicamente al personale espressamente autorizzato e sono registrate in un apposito giornale di controllo.

4. La data, l'ora e i minuti, iniziali e finali, di ogni intervallo di tempo nel quale i registri non risultano accessibili dall'esterno, oppure sono indisponibili in una loro funzionalità, sono registrate in un apposito giornale di controllo.

5. Almeno una copia dei registri è conservata in locali di sicurezza, ubicati in luoghi diversi da quelli ove sono custoditi gli originali.

Art. 19.

*Modalità di accesso ai registri degli indirizzi elettronici*

1. L'accesso ai registri degli indirizzi elettronici avviene secondo una modalità compatibile con il protocollo LDAP, definito nella specifica pubblica RFC 1777 e successive modificazioni.

2. Il gestore centrale dell'accesso e i punti di accesso possono fornire modalità di accesso al proprio registro aggiuntive, rispetto a quella prevista dal comma 1.

3. La struttura LDAP è specificata nei decreti ministeriali di cui all'art. 62, comma 2.

*Capo III*

ATTIVITÀ DEL SICI

Art. 20.

*Funzionamento e gestione del SICI*

1. La direzione generale per i sistemi informativi automatizzati del Ministero della giustizia (DGSIA) cura il funzionamento e la gestione del gestore centrale.

2. Il coordinamento interdistrettuale dei sistemi informativi automatizzati (CISIA) cura, attraverso l'amministratore di sistema, il funzionamento del gestore locale degli uffici di competenza.

3. Il dirigente amministrativo dell'ufficio giudiziario e dell'UNEP curano e sono responsabili, per l'ufficio di propria competenza, della consistenza dei dati.

Art. 21.

*Attività del gestore centrale*

1. Il gestore centrale fornisce il servizio di consultazione del SICI e il servizio di trasmissione telematica degli atti. I soggetti abilitati esterni accedono ai servizi del gestore centrale esclusivamente attraverso il proprio punto di accesso.

2. Il gestore centrale è connesso ai punti di accesso mediante canali sicuri.

3. Nelle comunicazioni o notificazioni al difensore, il gestore centrale controlla, mediante il registro generale degli indirizzi elettronici, la certificazione del difensore. In caso di esito negativo del controllo, il gestore centrale inoltra la comunicazione o notifica, e trasmette all'ufficio giudiziario o all'UNEP un messaggio contenente l'esito del controllo.

4. Il gestore centrale associa automaticamente, ad ogni documento informatico pervenuto da un punto di accesso, una attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti, che è inserita in un messaggio inviato all'indirizzo elettronico del mittente.

5. Il gestore centrale associa automaticamente, ad ogni ricevuta breve di avvenuta consegna pervenuta da un punto di accesso, una attestazione temporale, comprensiva di data, ora e minuti di ricezione del relativo documento informatico da parte del destinatario, e trasmette questi dati al gestore locale dell'ufficio giudiziario competente.

6. Il gestore centrale utilizza, per gli adempimenti di cui ai commi 4 e 5, un servizio di attestazione temporale basato, con una differenza non superiore ad un minuto primo, sulla scala di tempo UTC (IEN), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.

7. Il gestore centrale verifica l'assenza di virus informatici in ogni messaggio, in arrivo e in partenza.

8. Il gestore centrale, se riceve un messaggio privo dei dati necessari all'instradamento verso l'ufficio giudiziario o l'UNEP, genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio e l'indicazione degli elementi mancanti.

9. Il gestore centrale inoltra automaticamente tutti i documenti informatici provenienti dall'esterno del SICI e diretti verso il gestore locale dell'ufficio giudiziario o dell'UNEP, ed associa la attestazione temporale.

10. Il gestore centrale fornisce un servizio di inoltro automatico di tutti i documenti informatici ricevuti dall'interno del SICI verso l'indirizzo elettronico di destinazione.

11. Il gestore centrale fornisce il servizio di conservazione di tutti i messaggi inviati e ricevuti, associati alle relative attestazioni temporali, con le modalità previste dalla delibera CNIPA del 19 febbraio 2004, n. 11. I supporti sono inviati, con periodicità mensile, ad un apposito centro di conservazione presso il Centro di gestione centralizzata del Ministero della giustizia, che ne assicura la conservazione per un periodo non inferiore a cinque anni.

12. Il gestore centrale esegue la certificazione del difensore, qualora non sia già stata compiuta dal punto d'accesso.

13. Il gestore centrale fornisce un servizio per verificare lo stato delle notifiche e delle relative ricevute brevi di avvenuta consegna.

Art. 22.

*Attività del gestore locale*

1. Il gestore locale fornisce il servizio di consultazione del sistema informatico dell'ufficio giudiziario, per i soggetti abilitati, collegati attraverso il gestore centrale.

2. Il gestore locale, mediante il sistema informatico di gestione della cancelleria, fornisce il servizio di consultazione, nei limiti dei privilegi di accesso dell'utente.

3. Il gestore locale trasmette i documenti tra i sistemi informatici dell'ufficio giudiziario o dell'UNEP ed il gestore centrale.

4. Il gestore locale fornisce una verifica della ricezione di tutti i documenti informatici ricevuti dal gestore centrale e delle relative attestazioni temporali.

5. Il gestore locale decifra i messaggi crittografati ricevuti, secondo le regole previste all'art. 42.

6. Il gestore locale cifra, con le modalità di cui all'art. 43, i documenti in uscita, facenti parte del fascicolo informatico, quando sono destinati a soggetti abilitati esterni.

7. Il gestore locale verifica automaticamente, con il controllo della firma digitale, l'autenticità e l'integrità di ogni documento informatico ricevuto.

8. Il gestore locale verifica il rispetto dei formati e l'assenza di virus.

9. Il gestore locale rende disponibile il documento ricevuto al sistema informatico di gestione delle cancellerie civili o dell'UNEP, associandovi le informazioni dell'attività di verifica di cui al comma 8, per valutarne la ricevibilità.

Art. 23.

*Attività del sistema informatico di gestione della cancelleria*

1. Il sistema informatico di gestione delle cancellerie civili cura l'accettazione del documento ricevuto aggiornando il relativo registro ed il fascicolo informatico.

2. Il sistema informatico di gestione delle cancellerie civili invia, tramite il gestore locale ed il gestore centrale, all'indirizzo elettronico del mittente, una comunicazione di accettazione del documento informatico da parte della cancelleria oppure i motivi della mancata accettazione. La comunicazione contiene, se possibile, il numero di iscrizione a ruolo.

Art. 24.

*Attività del sistema informatico di gestione dell'UNEP*

1. Il sistema informatico di gestione degli UNEP acquisisce i documenti informatici da notificare, procede alla loro notifica e li restituisce con la relata di notifica.

Art. 25.

*Orario di disponibilità dei servizi*

1. Il gestore centrale ed i gestori locali garantiscono la disponibilità del servizio, nei giorni feriali, dalle ore otto alle ore ventitrè, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

Art. 26.

*Requisiti tecnici di sicurezza*

1. Al gestore centrale si applicano le regole di sicurezza stabilite per il SICI e per la RUG.

2. Per il gestore locale e per il fascicolo informatico si applicano le norme sulla sicurezza previste dal decreto del Ministero della giustizia del 24 maggio 2001.

Art. 27.

*Requisiti tecnici relativi all'infrastruttura di comunicazione*

1. Il gestore centrale ed i gestori locali comunicano, tra loro, esclusivamente mediante la RUG.

2. Il gestore centrale utilizza l'infrastruttura tecnologica resa disponibile nell'ambito della rete unitaria della pubblica amministrazione (RUPA) per le comunicazioni con l'esterno del dominio giustizia.

*Capo IV*

ACCESSO AL SICI

Art. 28.

*Funzionamento e gestione del punto di accesso*

1. Il funzionamento e la gestione dei punti di accesso è a carico dei soggetti pubblici o privati, in possesso dei requisiti di cui all'art. 6.

Art. 29.

*Funzionalità del punto di accesso*

1. Il punto di accesso fornisce ai soggetti abilitati esterni i servizi di consultazione del SICI e di trasmissione telematica degli atti.

2. Il punto di accesso fornisce il servizio di autenticazione dei soggetti abilitati, per l'accesso al SICI. Il

punto di accesso, gestito dal consiglio dell'ordine degli avvocati di appartenenza o dal Consiglio nazionale forense, con l'autenticazione del difensore, esegue la certificazione di cui all'art. 7.

3. La comunicazione tra la postazione informatica del soggetto abilitato esterno e il punto di accesso avviene mediante canale sicuro.

4. Il punto di accesso mantiene in linea i documenti informatici inviati fino a quando non riceve un avviso di consegna dal gestore centrale o dal punto di accesso di destinazione.

5. Il punto di accesso fornisce il servizio di ricezione, inviando, in risposta ad ogni documento informatico ricevuto dal gestore centrale o da un altro punto di accesso, una ricevuta breve di avvenuta consegna.

6. Il punto di accesso verifica l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.

7. Il punto di accesso garantisce, per un periodo non inferiore a cinque anni, la conservazione di tutti i messaggi inviati e ricevuti.

8. Il punto di accesso fornisce il servizio di distribuzione del software, fornito come prototipo dal Ministero della giustizia, per la redazione dei documenti informatici in formato XML.

Art. 30.

*Requisiti tecnici del punto di accesso*

1. L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche previste dalla carta nazionale dei servizi.

2. I punti di accesso stabiliscono le connessioni con il gestore centrale esclusivamente mediante un collegamento diretto alla RUPA, autorizzato dal CNIPA.

3. Ciascun punto di accesso stabilisce con il gestore centrale un canale sicuro di comunicazione, che consente la reciproca autenticazione e riservatezza.

4. Il punto di accesso garantisce un livello di disponibilità del servizio pari al 99,5 per cento, su base quadrimestrale, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

5. Le procedure per la fornitura dei servizi attuate dal punto di accesso sono dettagliatamente documentate sul manuale operativo, previsto dall'art. 33.

6. Tutte le azioni e le procedure di sicurezza attivate dal punto di accesso sono dettagliatamente documentate nel piano per la sicurezza, previsto dall'art. 34.

7. La frequenza di salvataggio dei dati è almeno giornaliera.

8. Gli eventi significativi nel funzionamento del punto di accesso, sono registrati sul giornale di controllo, di cui all'art. 35.

9. I canali di autenticazione del presente regolamento sono in SSL versione 3, con chiave a 1024 bit.

Art. 31.

*Elenco pubblico dei punti di accesso*

1. L'elenco pubblico dei punti di accesso, attivo presso il Ministero della giustizia, comprende le seguenti informazioni:

*a)* identificativo del punto di accesso;

*b)* sede legale del soggetto titolare del punto di accesso;

*c)* nome secondo lo standard X.500;

*d)* indirizzo Internet;

*e)* dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo elettronico, numero di telefono e di fax;

*f)* elenco dei numeri telefonici di accesso;

*g)* manuale operativo;

*h)* data di cessazione dell'attività.

Art. 32.

*Iscrizione nell'elenco pubblico dei punti di accesso*

1. Il soggetto che intende costituire un punto di accesso inoltra, alla DGSIA, domanda di iscrizione nell'elenco pubblico dei punti di accesso.

2. Alla domanda sono allegate le dichiarazioni di:

*a)* possesso dei requisiti di cui all'art. 6;

*b)* attestazione di affidabilità organizzativa e tecnica necessaria per svolgere il servizio di punto di accesso;

*c)* attestazione relativa all'impiego di personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti;

*d)* obbligo di fornirsi di: manuale operativo, piano per la sicurezza e giornale di controllo, secondo quanto previsto dagli articoli 33, 34 e 35;

*e)* obbligo di garantire la sicurezza e l'integrità del servizio e dei dati di propria competenza;

*f)* obbligo di compiere il processo di autenticazione dei soggetti abilitati ad esso afferenti, su mandato del Ministero della giustizia, conformemente all'art. 30, comma 1;

*g)* obbligo di comunicare, al Ministero della giustizia, la data di cessazione del servizio, con preavviso di sei mesi;

*h)* informazione dei dati di cui all'art. 31.

3. Il Ministero della giustizia decide sulla domanda, con provvedimento motivato, anche sulla base di apposite verifiche, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente.

4. Con il provvedimento di cui al comma 3, il Ministero della giustizia delega la responsabilità del processo di autenticazione dei soggetti abilitati esterni al punto di accesso.

5. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del

punto di accesso, di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'art. 6, comma 3.

Art. 33.

*Manuale operativo*

1. Il punto di accesso utilizza un manuale operativo in cui sono definite le procedure applicate per effetto del presente decreto.

2. Il manuale operativo è pubblicato a cura del punto di accesso, per la consultazione in via telematica.

3. Il manuale operativo contiene almeno le seguenti informazioni:

*a)* dati identificativi del punto di accesso e del relativo gestore;

*b)* dati identificativi della versione del manuale operativo;

*c)* responsabile del manuale operativo;

*d)* definizione degli obblighi del titolare del punto di accesso e di coloro che vi accedono per l'utilizzo dei servizi;

*e)* definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;

*f)* tariffe;

*g)* modalità di autenticazione, registrazione e gestione degli utenti;

*h)* modalità di attivazione e gestione degli indirizzi elettronici;

*i)* modalità di gestione del registro degli indirizzi elettronici;

*j)* modalità di accesso al registro degli indirizzi elettronici;

*k)* politiche e procedure di sicurezza.

Art. 34.

*Piano per la sicurezza*

1. Il punto di accesso individua ed iscrive, nel giornale di controllo, il responsabile per la sicurezza.

2. Il responsabile di cui al comma 1 definisce il piano per la sicurezza che contiene almeno i seguenti elementi:

*a)* struttura generale, modalità operativa e struttura logistica dell'organizzazione;

*b)* descrizione dell'infrastruttura di protezione per ciascun immobile rilevante ai fini della sicurezza;

*c)* collocazione dei servizi e degli uffici negli immobili dell'organizzazione;

*d)* elenco del personale e sua distribuzione negli uffici;

*e)* ripartizione e definizione delle responsabilità;

*f)* descrizione delle procedure utilizzate nell'attività di attivazione delle utenze e, limitatamente ai punti di accesso, di rilascio di indirizzi elettronici;

*g)* descrizione dei dispositivi installati;

*h)* descrizione dei flussi di dati;

*i)* procedura di gestione delle copie di sicurezza dei dati;

*j)* procedura di gestione dei disastri;

*k)* analisi dei rischi;

*l)* descrizione delle contromisure;

*m)* specificazione dei controlli.

3. Il piano per la sicurezza è conforme a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, e può essere adottato unitamente al documento programmatico per la sicurezza previsto dall'art. 34, comma 1, lettera *g)*, del medesimo decreto legislativo.

Art. 35.

*Giornale di controllo*

1. Il punto di accesso attiva il giornale di controllo, contenente l'insieme delle registrazioni effettuate automaticamente allorché si verificano le condizioni previste dal presente decreto.

2. Le registrazioni possono essere effettuate in modo indipendente, anche su distinti supporti e di diverso tipo.

3. La registrazione associa la data, l'ora e i minuti in cui è effettuata.

4. Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e da consentire la ricostruzione accurata di tutti gli eventi rilevanti per la sicurezza.

5. L'integrità del giornale di controllo è verificata con frequenza almeno mensile.

6. Le registrazioni contenute nel giornale di controllo sono archiviate con le modalità previste dal presente decreto e conservate per un periodo non inferiore a cinque anni.

Art. 36.

*Postazioni di lavoro dei soggetti abilitati esterni*

1. La postazione di lavoro dei soggetti abilitati esterni è l'insieme delle risorse hardware, software e di rete da loro utilizzate direttamente per la formazione dei documenti informatici, per l'inoltro e la ricezione dei messaggi e per la consultazione del SICI.

2. La postazione di lavoro dei soggetti abilitati esterni è dotata dell'hardware e del software necessario alla gestione della firma digitale su smartcard, e all'autenticazione nei confronti del punto di accesso, secondo le caratteristiche tecniche della carta nazionale dei servizi.

3. La postazione di lavoro dei soggetti abilitati esterni è dotata di software idoneo a verificare l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.

*Capo V*

TRASMISSIONE DI DOCUMENTI INFORMATICI TRA IL SICI ED ENTITÀ ESTERNE

Art. 37.

*Principi normativi*

1. Nella trasmissione di documenti informatici nell'ambito del processo civile, trovano applicazione tutte le prescrizioni contenute nel decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nel decreto legislativo 23 gennaio 2002, n. 10, e successive modificazioni.

2. I documenti informatici prodotti nel processo civile sono sottoscritti con firma digitale, nei casi previsti dall'art. 4, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123.

Art. 38.

*Ricezione del documento informatico*

1. Il documento informatico inviato da un soggetto abilitato esterno è ricevuto dal SICI nel momento in cui il gestore centrale lo accetta e associa l'attestazione temporale di cui all'art. 21, comma 4.

2. Il documento informatico inviato da un soggetto abilitato interno è ricevuto, dal soggetto abilitato esterno, nel momento in cui il gestore centrale riceve la ricevuta breve di avvenuta consegna relativa al documento e associa l'attestazione temporale di cui all'art. 21, comma 5.

Art. 39.

*Orario dei servizi telematici di cancelleria*

1. Il SICI fornisce i servizi telematici di cancelleria, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

Art. 40.

*Iscrizione a ruolo generale*

1. Il sistema informatico dell'ufficio giudiziario invia al difensore, che iscrive la causa a ruolo per via telematica, una comunicazione, recante il numero di ruolo del procedimento assegnato dall'ufficio.

Art. 41.

*Dimensione del messaggio*

1. La dimensione massima del messaggio è di 10 Mb.

Art. 42.

*Crittografia del messaggio*

1. Al fine della riservatezza del documento da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia basato sulla chiave pubblica del gestore locale cui è destinato il messaggio.

2. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato *A* del presente decreto.

3. Le chiavi pubbliche dei gestori locali sono pubblicate in un registro del gestore centrale dell'accesso.

4. Il registro di cui al comma 3 è accessibile in modalità LDAP.

Art. 43.

*Trasmissione e consultazione dei fascicoli*

1. Nel caso di richiesta di trasmissione o di consultazione, totale o parziale, di un fascicolo, il gestore locale, per garantire la riservatezza della comunicazione, utilizza un meccanismo di crittografia basato sulla chiave pubblica di cifratura del soggetto abilitato esterno di destinazione.

2. Nel caso di richiesta di copia conforme del fascicolo, totale o parziale, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.

3. Le chiavi pubbliche dei soggetti abilitati esterni sono disponibili nel registro generale degli indirizzi di cui all'art. 13.

4. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato *A*, del presente decreto.

Art. 44.

*Trasmissione delle sentenze*

1. L'originale della sentenza, redatta in formato elettronico dal giudice estensore o, ai sensi dell'art. 119 delle norme di attuazione del codice di procedura civile, dal cancelliere o dal dattilografo da questi incaricato, è sottoscritta con firma digitale dall'estensore, previa verifica della conformità dell'originale alla minuta.

2. In caso di giudice collegiale, l'originale della sentenza è sottoscritto con firma digitale anche dal presidente e, a tal fine, la sentenza gli è trasmessa, in formato elettronico, dal giudice estensore o dal cancelliere.

3. Il cancelliere attesta il deposito della sentenza apponendo la data e sottoscrivendo la sentenza con la propria firma digitale.

Art. 45.

*Comunicazioni e notificazioni*

1. La comunicazione per via telematica di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno avviene mediante inoltro del documento dal gestore locale al gestore centrale, che lo invia alla CPECPT del destinatario.

3. La notificazione telematica di documenti informatici tra difensori avviene, ove sussistano i presupposti di cui alla legge 21 gennaio 1994, n. 53, mediante inoltro del documento dal punto di accesso del mittente alla CPECPT del destinatario. A tale scopo il punto di

accesso trasmette il messaggio con il documento da notificare al gestore centrale che, a sua volta, inoltra il messaggio ricevuto al punto di accesso di destinazione.

3. Le richieste di un'attività di notifica telematica da parte di un ufficio giudiziario sono inoltrate, mediante la RUG, al sistema informatico dell'UNEP. Le richieste dei difensori sono inoltrate all'UNEP per il tramite del punto di accesso del mittente e del gestore centrale, nel rispetto dei requisiti dei documenti informatici provenienti dall'esterno. La notificazione di documenti informatici da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da ufficio giudiziario verso soggetti abilitati esterni.

4. Il sistema informatico dell'UNEP, eseguita la notifica, trasmette per via telematica, a chi ha richiesto il servizio, il documento informatico con la relata di notifica, costituita dalla ricevuta elettronica, sottoscritta dall'ufficiale giudiziario con firma digitale.

5. Nell'ipotesi di cui all'art. 6, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, l'ufficiale giudiziario provvede a notificare il duplicato del documento informatico, su supporto ottico non riscrivibile.

6. La consegna del documento informatico alla CPECPT del soggetto abilitato esterno è assicurata dai punti di accesso mediante l'invio al mittente di una ricevuta breve di avvenuta consegna.

7. Il gestore centrale, nella trasmissione di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno, associa automaticamente ad ogni ricevuta breve di avvenuta consegna una attestazione temporale contenente data, ora e minuti della ricezione che inoltra al gestore locale per l'inserimento nel fascicolo informatico.

8. Nelle notifiche tra difensori, il gestore centrale, ricevuto dal mittente il messaggio da notificare, associa automaticamente ad esso una prima attestazione temporale, che viene spedita alla CPECPT del mittente e, unitamente al messaggio, alla CPECPT del destinatario. La CPECPT del destinatario, ricevuto il messaggio, invia al gestore centrale la ricevuta breve di avvenuta consegna; il gestore centrale associa a quest'ultima una seconda attestazione temporale, che viene spedita alla CPECPT del destinatario e, unitamente alla ricevuta breve di avvenuta consegna, alla CPECPT del mittente.

### *Capo VI*

### Pagamenti

#### Art. 46.

*Pagamenti*

1. I pagamenti per via telematica, relativi agli atti giudiziari, si effettuano mediante il modello definito dal Ministero dell'economia e delle finanze.

2. Il pagamento può anche avvenire nelle forme di cui all'art. 1 del decreto del Presidente della Repubblica del 1° marzo 2001, n. 126.

3. Gli estremi del pagamento sono allegati alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio giudiziario.

4. Se il pagamento è effettuato a norma del comma 2 e con sistemi non telematici, l'originale cartaceo dell'attestazione di pagamento deve, in ogni caso, essere presentato per la prima udienza.

#### Art. 47.

*Diritto di copia*

1. Il difensore nella richiesta di copia può chiedere l'indicazione dell'importo del diritto corrispondente che gli è comunicato, senza ritardo, dall'ufficio giudiziario.

2. Alla richiesta di copia è associato un numero identificativo che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel fascicolo informatico per consentire il versamento secondo le modalità previste dal decreto del Presidente della Repubblica 1° marzo 2001, n. 126.

#### Art. 48.

*Registrazione, trascrizione e voltura degli atti*

1. La registrazione, la trascrizione e la voltura degli atti avvengono, in via telematica, nelle forme previste dall'art. 73 del decreto del Presidente della Repubblica 30 maggio 2002, n. 115.

#### Art. 49.

*Pagamento dei diritti di notifica*

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'art. 46.

2. L'UNEP rende pubblici, attraverso il gestore locale dell'ufficio, gli importi dovuti a titolo di anticipazione. Eseguita la notifica, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previa definizione del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.

### *Capo VII*

### Archiviazione e conservazione delle informazioni

#### Art. 50.

*Gestione del fascicolo informatico*

1. Il sistema di gestione del fascicolo informatico è la parte del sistema dell'ufficio giudiziario dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno dell'ufficio giudiziario.

2. Il fascicolo informatico contiene i documenti informatici e le relative informazioni quali: allegati, ricevute brevi di avvenuta consegna e attestazioni temporali.

Art. 51.

*Archiviazione e conservazione dei documenti informatici degli uffici giudiziari e degli UNEP*

1. I fascicoli informatici relativi ai procedimenti in corso sono archiviati, per tutta la durata del procedimento, nell'archivio in linea dell'ufficio giudiziario, secondo le modalità previste dal decreto ministeriale del 24 maggio 2001 e dal decreto legislativo 30 giugno 2003, n. 196.

2. I fascicoli informatici relativi ai procedimenti esauriti sono soggetti a conservazione, presso il competente ufficio giudiziario, secondo le modalità previste dalla deliberazione del CNIPA del 19 febbraio 2004, n. 11, per il periodo previsto dall'art. 41 del decreto legislativo 22 gennaio 2004, n. 42, fatte salve le operazioni di scarto ivi previste.

3. I documenti informatici degli UNEP sono soggetti a conservazione, presso il competente ufficio, secondo le modalità e termini di cui al comma 2.

*Capo VIII*

STANDARD E MODELLI DI RIFERIMENTO

Art. 52.

*Formato dei documenti informatici*

1. Gli atti del processo in forma di documenti informatici sono redatti in formato XML, le cui specifiche tecniche sono determinate a norma dell'art. 62, comma 2.

Art. 53.

*Formato dei documenti informatici allegati*

1. I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, ed hanno i seguenti formati: .pdf, .rtf, .txt, .jpg, .gif, .tiff, .xml.

2. È consentito l'utilizzo dei formati compressi .zip, .rar. e .arj, purché contenenti file nei formati previsti dal comma precedente.

Art. 54.

*Documenti probatori e allegati non informatici*

1. I documenti probatori e gli allegati depositati in formato non elettronico, sono identificati e descritti in una apposita sezione del documento informatico, secondo la definizione del modello DTD (Document Type Definition) e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati: numero di ruolo della causa, progressivo dell'allegato e indicazione della prima udienza successiva al deposito.

Art. 55.

*Servizio di posta elettronica*

1. Il servizio di posta elettronica utilizzato dal gestore centrale dell'accesso e dai punti di accesso è conforme agli standard dei sistemi di posta elettronica compatibili con il protocollo di trasporto SMTP ed il formato dei messaggi S/MIME.

Art. 56.

*Modelli di documenti informatici prodotti dai difensori*

1. I modelli dei documenti informatici prodotti dai difensori, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

*a)* atto introduttivo (citazione, ricorso, ricorso cautelare, ricorso per decreto ingiuntivo);

*b)* nota di iscrizione a ruolo;

*c)* comparsa di costituzione e risposta con eventuale domanda riconvenzionale ed eventuale richiesta di rinvio della prima udienza per la chiamata in causa del terzo;

*d)* deduzioni istruttorie a norma dell'art. 184 del codice di procedura civile;

*e)* note autorizzate ex art. 183, comma 5, del codice di procedura civile;

*f)* memorie autorizzate;

*g)* chiamata in causa del terzo;

*h)* istanza;

*i)* reclamo;

*j)* atti conclusivi (comparsa conclusionale, memoria di replica);

*k)* atto di pignoramento;

*l)* atto di intervento nell'esecuzione;

*m)* osservazioni al progetto di distribuzione;

*n)* istanza di fallimento;

*o)* istanza di insinuazione al passivo;

*p)* ricorso per insinuazione tardiva;

*q)* ricorso per opposizione allo stato passivo;

*r)* istanza di ammissione alla procedura di amministrazione controllata;

*s)* istanza di ammissione alla procedura di concordato preventivo;

*t)* istanza di concordato fallimentare;

*u)* dichiarazione di voto nelle procedure di amministrazione controllata o di concordato;

*v)* delega rilasciata ai sensi dell'art. 9 del regio decreto legislativo 27 novembre 1933, n. 1578.

Art. 57.

*Modelli di documenti informatici prodotti dalla cancelleria*

1. I modelli dei documenti informatici prodotti dalla cancelleria, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

*a)* verbale di udienza;

*b)* biglietto di cancelleria;

*c)* richiesta di notifica;

*d)* richiesta di informazione o ordine di esibizione.

Art. 58.

*Modelli di documenti informatici prodotti dal giudice*

1. I modelli dei documenti informatici prodotti dal giudice, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

*a)* provvedimento (sentenza, ordinanza, decreto);

*b)* dispositivo sentenza;

*c)* verbale di conciliazione.

Art. 59.

*Modelli di documenti informatici prodotti dal consulente tecnico di ufficio*

1. I modelli dei documenti informatici prodotti dal consulente tecnico di ufficio, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

*a)* modello generico di consulenza;

*b)* stima di beni mobili;

*c)* stima di beni immobili;

*d)* stima di azienda.

Art. 60.

*Modelli di documenti informatici prodotti dall'UNEP*

1. Il modello dei documenti informatici prodotti dall'UNEP, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi al seguente atto: relata di notifica.

*Capo IX*

DISPOSIZIONI FINALI E TRANSITORIE

Art. 61.

*Adeguamento delle regole tecnico-operative*

1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.

Art. 62.

*Disposizioni transitorie*

1. L'attivazione del processo telematico è preceduta da un decreto dirigenziale, che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.

2. Le caratteristiche specifiche della strutturazione dei modelli DTD (Document Type Definition) saranno pubblicate, con uno o più decreti ministeriali, entro 180 giorni dalla data di entrata in vigore del presente decreto.

3. Fino all'entrata in vigore delle regole tecniche relative alla carta nazionale dei servizi, l'autenticazione dei soggetti abilitati esterni avviene mediante dispositivo di crittografia contenente al suo interno un certificato di autenticazione e la corrispondente chiave privata protetta da PIN. La chiave privata, lunga almeno 1024 bit e generata all'interno del dispositivo crittografico, non deve essere estraibile dal dispositivo stesso.

4. L'art. 22, comma 6, e l'art. 43, comma 1, hanno efficacia a decorrere da sei mesi dalla data di entrata in vigore del presente decreto.

Roma, 14 ottobre 2004

*Il Ministro:* CASTELLI

ALLEGATO *A*

# ***REGOLE TECNICO-OPERATIVE***

*PER L'USO DI STRUMENTI INFORMATICI E TELEMATICI*
*NEL PROCESSO CIVILE*

INDICE

## DEFINIZIONI E ACRONIMI

Nel presente capitolo è riportata la descrizione dei termini, degli acronimi e delle abbreviazioni usate nel documento.

| *Acronimo* | *Descrizione* |
|---|---|
| CdO | Consiglio dell'Ordine |
| CPECPT | Casella di Posta Elettronica Certificata Processo Telematico |
| DTD | Document Type Definition |
| GC | Gestore Centrale |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| MIME | Multipurpose Internet Mail Extensions |
| PCT | Processo Civile Telematico |
| PdA | Punto di Accesso |
| PIN | Personal Identification Number |
| RDPIC | Ricevuta di presa in carico |
| ReGIndE | Registro Generale degli Indirizzi Elettronici |
| ReLIndE | Registro Locale degli Indirizzi Elettronici |
| RPC | Remote Procedure Call |
| RUG | Rete Unica della Giustizia |
| RUPA | Rete Unitaria della Pubblica Amministrazione |
| S/MIME | Secure Multipurpose Internet Mail Extensions |
| SIC | Sistema Informativo Civile |
| SICC | Sistema Informatico del Contenzioso Civile |
| SIL | Sistema Informativo del Lavoro |
| SMTP | Simple Mail Transfer Protocol |
| SOAP | Simple Object Access Protocol |
| SPC | Servizio Pubblico di Connessione |
| SSLv3 | Secure Sockets Layer version 3 |
| UG | Ufficio Giudiziario |
| UNEP | Ufficio Notifiche e Protesti |
| W3C | World Wide Web Consortium |
| XML | eXtensible Markup Language |

# 1 DESCRIZIONE DELL'ARCHITETTURA DEL SISTEMA

## *1.1 SCENARIO COMPLESSIVO ED ATTORI COINVOLTI*

Il Processo telematico prevede il seguente scenario operativo:

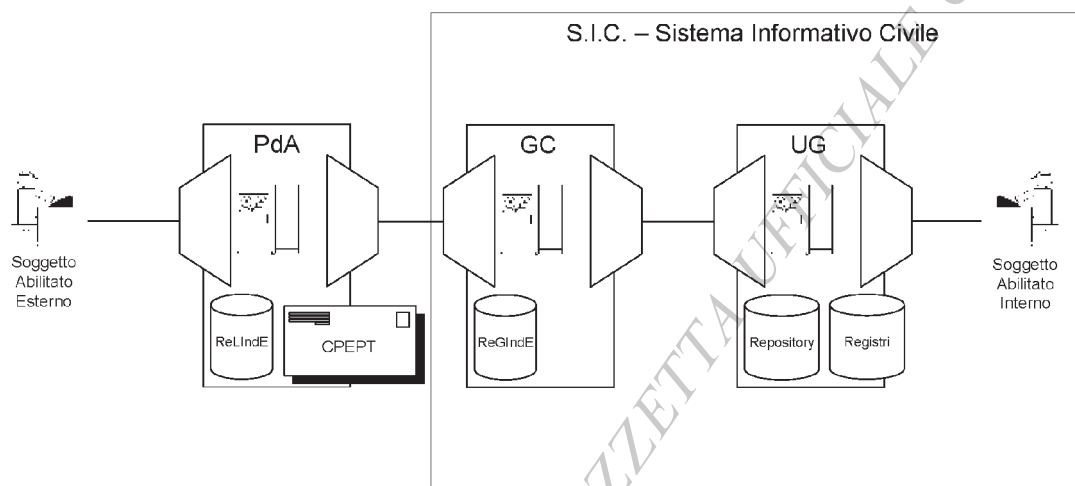



***Figura 1 – Scenario operativo di riferimento***

Dove:

- PdA = Punto di accesso
- GC = Gestore centrale
- UG = Ufficio Giudiziario

Nella fase 1.0 di sperimentazione, il contesto applicativo, oggetto di analisi e realizzazione, sarà limitato al solo Sistema Informativo del Contenzioso Civile (SICC) presso i Tribunali Ordinari; i Soggetti Abilitati Esterni saranno limitati ai soli Avvocati.

L'Avvocato può, già a partire dalla prima fase sperimentale (fase 1.0):

- redigere e firmare l'atto di parte: a tal fine si avvale di uno strumento di redazione (Redattore Atti) integrato con strumenti *software* per la firma, cifratura e imbustamento;
- depositare l'atto di parte (ricevendo la relativa attestazione temporale e successivamente la ricevuta elettronica di avvenuta presa in carico da parte dell'Ufficio Giudiziario);
- ricevere comunicazioni da parte dell'Ufficio Giudiziario nella propria "Casella di Posta Elettronica Certificata del Processo Telematico" (CPECPT);
- effettuare consultazioni dei fascicoli di propria pertinenza tramite l'evoluzione del PolisWeb (sito internet di consultazione disponibile agli avvocati abilitati).

L'Avvocato interagisce con il S.I.C. necessariamente per il tramite di un **Punto di Accesso Esterno** (PdA), presso cui è registrato come utente nel Registro Locale degli Indirizzi

Elettronici (ReLIndE).

Il PdA è quindi l'unico fornitore dei servizi di interfacciamento del "dominio giustizia" per gli Avvocati, autorizzato ad operare su provvedimento dell'Amministrazione. Questo in quanto offre ai propri Utenti una schermatura dei protocolli e dei formati di interfaccia previsti dal PCT per il colloquio con gli Uffici Giudiziari (UG), salvaguardando i principi di sicurezza e di riservatezza (tramite **autenticazione forte**) alla base della specifica problematica applicativa.

Presso il PdA è attivo un Registro Locale degli Indirizzi Elettronici (ReLIndE), che viene acceduto in fase di autenticazione, in fase di prelievo o consultazione dei messaggi provenienti dal SIC e in fase di deposito degli atti, per eseguire, se in possesso dell'albo elettronico del Consiglio dell'Ordine di appartenenza dell'Avvocato, la certificazione dello status del professionista.

Per quanto attiene alla ricezione di comunicazioni di cancelleria, il PdA fornirà all'avvocato una casella di posta elettronica certificata in aderenza alle specifiche dettate dal Centro Tecnico della RUPA, opportunamente adattate per il Processo Telematico.

Il **Gestore Centrale** (GC) svolge servizi di cooperazione allo scambio di dati che, pur non entrando nel merito delle richieste ricevute, consentono di assicurare la correttezza della composizione delle buste prodotte e di tracciare tutti i flussi applicativi, verificando il completamento dei relativi cicli logici.

Provvede cioè ad indirizzare le richieste inoltrate dai PdA, e originate dagli Avvocati, verso gli UG destinatari e viceversa a smistare ai relativi PdA le risposte o le comunicazioni provenienti dagli UG, sopperendo, grazie ad una architettura logica e fisica particolarmente robusta, alla eventuale indisponibilità temporanea dei relativi sistemi di colloquio.

Il GC associa automaticamente , ad ogni documento informatico pervenuto da un punto di accesso, un' attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti. Questa è inserita in un messaggio inviato alla casella di posta elettronica di servizio del Punto di Accesso, che provvede a renderla disponibile al mittente.

Il GC esegue inoltre, in fase di deposito di un atto, la certificazione sostitutiva del difensore, nei casi in cui il PdA mittente non sia tenuto, o non sia stato delegato, alla gestione dell'albo dell'Ordine professionale di appartenenza dell'Avvocato mittente. A tal fine è previsto che ciascun Consiglio dell'Ordine inoltri al GC l'elenco aggiornato dei propri iscritti all'albo.

L'entità rappresentata come Ufficio Giudiziario coincide tecnicamente con il cosiddetto **Gestore Locale**, ossia l'insieme di tutti i servizi applicativi del Processo Telematico esposti sia verso il Gestore Centrale sia verso i soggetti abilitati ed i sistemi interni.

In particolare all'interno di questa componente vengono realizzati tutti i sottosistemi per:

- la gestione delle fasi di controllo e accettazione dell'atto di parte;
- l'invio di eventuali eccezioni al mittente;
- la gestione dei diritti di visibilità sui dati;
- l'invio dei biglietti di cancelleria.

Il Gestore Locale gestisce, infine, l'interfacciamento tra il *Repository* Documentale (la base dati documentale, contenente tra l'altro il fascicolo informatico) e il SICC (gestione registri del Contenzioso Civile) per tutto ciò che concerne le operazioni a disposizione dei soggetti abilitati interni.

L'operatore di cancelleria e il Magistrato si interfacciano alle funzionalità del Processo Telematico attraverso l'applicativo SICC. Le evoluzioni del SICC permetteranno infatti l'accesso al fascicolo informatico non più solo come storico degli eventi, ma anche nel merito del contenuto degli atti di parte.

Il Cancelliere in particolare, potrà intervenire, attraverso componenti specifiche previste dalle evoluzioni del SICC, per gestire le eventuali situazioni di eccezione che si possono verificare in fase di ricezione, controllo e accettazione degli atti di parte.

## *1.2 BREVI CENNI ARCHITETTURALI*

I flussi del Processo Telematico possono essere classificati per tipologia in invii documentali e consultazioni.

Dal punto di vista applicativo, la loro principale differenza è legata all'utilizzo di un differente protocollo di trasporto nella tratta tra PdA e GC. In particolare, per gli invii documentali, è previsto l'utilizzo di un meccanismo asincrono, basato sul protocollo SMTP, mentre per le consultazioni, si prevede l'utilizzo di soli meccanismi sincroni, basati su HTTPS.

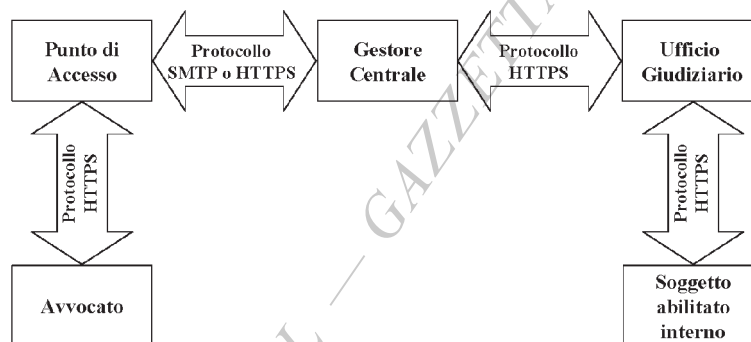



***Figura 2 – Protocolli di trasporto***

Gli Avvocati dovranno essere dotati di *smart card* contenenti:

- il certificato per la firma elettronica, rilasciato da un certificatore accreditato, in modo da garantire che quelle determinate credenziali siano riferite ad una persona fisica la cui identità è garantita dall'insieme dei processi di identificazione attuati dal certificatore stesso;
- il certificato di autenticazione, per la connessione al Punto di Accesso, rilasciato da una certification authority riconosciuta dal Punto di Accesso.

Sarà pertanto possibile l'utilizzo di una sola smart-card contenente entrambi i certificati oppure l'utilizzo di smart-card distinte. Sarà inoltre possibile dotarsi di più smart-card di autenticazione.

L'avvocato dovrà essere dotato inoltre di un certificato di crittografia necessario per decifrare gli atti criptati; questo dovrà avere lunghezza di chiave di almeno 1024 bit e potrà coincidere con il certificato di autenticazione.

Dal punto di vista pratico, dunque, gli Avvocati opereranno su *client* dotati di dispositivo di lettura della *smart card* e, nel momento di connessione al PdA, per il deposito o la consultazione, inseriranno il proprio PIN e presenteranno le proprie credenziali con cui verranno autenticati dal servizio, creando così un canale sicuro basato su protocollo SSLv3.

Gli UG saranno inoltre dotati di chiave e certificati di cifratura[1] per consentire che gli atti depositati vengano cifrati sul *client* dell'avvocato, con il certificato pubblico dell'UG destinatario, e che solo quest'ultimo possa procedere a decifrare e leggere gli atti stessi.

I PdA e il GC sono attestati su rete pubblica (SPC) e specificatamente su Interdominio RUPA; pertanto l'interazione tra le due entità, tanto in caso di utilizzo del protocollo sincrono (per le consultazioni dei procedimenti giudiziari) che asincrono (per gli invii documentali), fruisce delle garanzie di sicurezza offerta da tale rete. La tratta GC - UG sfrutta la Rete Unica della Giustizia (RUG).

In entrambi i casi si ipotizza comunque di instaurare sui protocolli sincroni una connessione sicura (SSLv3) mediante mutua autenticazione dei *server*.

## *1.3 SOTTOSISTEMI DISPONIBILI ALL'ESTERNO PER LA SPERIMENTAZIONE*

Nel seguente paragrafo sono riportati i sottosistemi resi disponibili dall'Amministrazione ai soli fini di consentire la sperimentazione presso le sedi pilota.

Relativamente a tutti questi moduli software, l'Amministrazione, nell'ambito delle regole tecnico-operative, fornisce le necessarie specifiche (WSDL, DTD e quant'altro) per consentire a tutti i fornitori di software l'integrazione dei loro software con i servizi del Processo Telematico secondo la logica "application-to-application".

***Stazione di lavoro dell' Avvocato*** È il sottosistema contenente l'insieme delle funzionalità fornite all'Avvocato al fine di consentirgli di compilare un atto, firmarlo digitalmente, criptarlo per l'UG di destinazione ed inoltrarlo al PdA di riferimento. A tale scopo si fornisce uno strumento di redazione atti, funzionalità per la firma e la crittografia e funzionalità per la spedizione, previa autenticazione ad un Punto di Accesso. Tale sottosistema consente di implementare i requisiti di strutturazione degli atti e la loro formattazione nello standard XML, secondo le specifiche che saranno riportate nelle Regole Tecniche.

***Punto di Accesso (PdA)*** E' il sottosistema attraverso il quale l'Avvocato può interagire con il Sistema Informatico Civile. Per il tramite di apposite funzionalità, il PdA consente all'utente di:

- depositare atti presso un Ufficio Giudiziario e di ricevere i relativi messaggi di risposta da parte del SIC;
- ricevere nella CPECPT di un Avvocato un biglietto di cancelleria generato da un Ufficio Giudiziario, emettendo le ricevute previste dagli standard di posta certificata;
- accedere, tramite Polis Web, alle informazioni tenute dagli Uffici Giudiziari in termini di consultazione dei dati relativi ai fascicoli di competenza. Nell'ambito di tale sottosistema è oggetto di fornitura il solo front-end dell'applicazione PolisWeb, attivabile a seguito dell'autenticazione dell'utente al PdA.

[1] Si ipotizza che l'Amministrazione assuma in proprio la responsabilità della produzione e della distribuzione dei certificati server validi limitatamente alla operatività del Processo Telematico (in questo modo, ad esempio, potrebbero risultare più gestibili le problematiche di rinnovo dei certificati).

*Sempre nella logica "application-to-application", le regole tecnico-operative forniscono le specifiche affinché ogni PdA fornito da terze parti possa costruirsi il proprio front-end per le consultazioni web, in eventuale sostituzione di PolisWeb (vedi sotto).*

***PolisWEB - Strumento di consultazione WEB*** E' il sottosistema costituito dall'applicazione per la consultazione Web delle informazioni contenute nei registri dei procedimenti, in ambiente SICC, e/o nei documenti afferenti ad un procedimento, in ambiente repository documentale. PolisWeb può essere utilizzato sia in ambiente Intranet (all'interno dell'UG, attraverso appositi "chioschi" informativi) che in ambiente Internet (attraverso il PdA).

## *1.4 FLUSSI PRINCIPALI*

Il presente paragrafo descrive i principali flussi del sistema, rappresentando le interazioni tra le principali componenti di ciascun sottosistema, seguendo l'iter logico della redazione e del deposito di un atto.

### *1.4.1 Redazione dell'atto di parte*

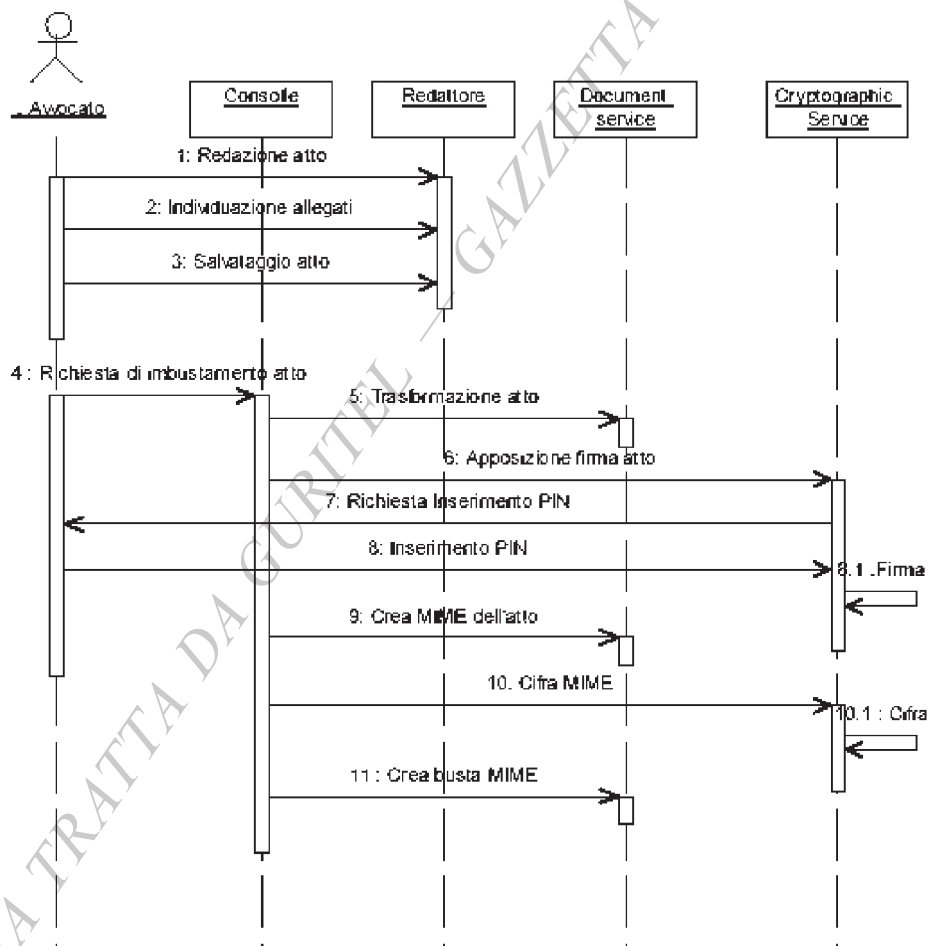



***Figura 3 – Sequence diagram redazione e imbustamento atto***

Nella Figura 3 è rappresentato il diagramma di sequenza relativo alla redazione dell'atto da parte dell'Avvocato e alla richiesta di imbustamento (necessario al successivo deposito dell'atto attraverso il PdA).

In particolare sono svolte le seguenti azioni:

1. L'avvocato scrive l'atto attraverso l'ambiente di redazione.
2. Individua i documenti da allegare all'atto.
3. Salva l'atto.
4. Al termine della redazione, dalla Consolle, l'Avvocato richiede l'imbustamento dell'atto.
5. L'atto viene convertito automaticamente in formato XML.

   *L'atto potrà essere visualizzato e stampato, utilizzando un visualizzatore che aderisce allo standard Formatting Objects. È opportuno infatti far presente che questa sarà la visualizzazione "ufficiale", consigliata all'avvocato soprattutto per la stampa, in quanto la trasformazione da Word a XML potrebbe non essere fedele al 100%.*

6. Viene richiesta l'operazione di firma dell'atto.
7. Viene richiesto all'Avvocato di inserire il PIN
8. L'Avvocato inserisce il PIN della Smartcard contenente il certificato digitale di firma.

   8.1 L'atto viene firmato

9. Viene creata la busta MIME dell'atto.
10. Viene richiesta l'operazione di cifratura del MIME dell'atto

    10.1 L'atto viene cifrato.

11. Viene creata la busta MIME contenente l'atto cifrato e le informazioni di instradamento all'UG.

A questo punto la busta è pronta per essere trasmessa attraverso la funzione di "deposito atto" messa a disposizione dal PdA.

Per attivare la funzione di "deposito atto" l'Avvocato si connette via internet con il proprio PdA, si autentica tramite smart-card e attiva la funzionalità di "deposito atto" che consente la trasmissione al PdA della busta memorizzata sulla postazione client.

La funzione di "deposito atto" prevede un flusso di trasmissione dell'atto informatico dal client dell'Avvocato che lo ha predisposto fino all'UG destinatario, cui farà seguito un messaggio di risposta da parte dell'UG per segnalare l'esito dell'atto depositato.

È inoltre previsto un ulteriore messaggio di risposta generato dal GC al momento della ricezione della richiesta di inoltro dell'atto all'UG. Tale risposta dipenderà dall'esito dei controlli eseguiti dal GC sulla busta inoltrata dal PdA. In caso di esito positivo detta risposta conterrà l'attestazione temporale dell'evento di ricezione della richiesta di deposito e la sua data di emissione avrà valore legale per la verifica dei termini di scadenza per la presentazione dell'atto, salvo verifica di buon fine dell'atto medesimo presso l'UG (verifica delle condizioni minime di accettabilità dell'atto). In caso di esito negativo, la risposta conterrà la segnalazione dell'errore riscontrato e bloccherà l'inoltro dell'atto all'UG.

A tale flusso collaborano:

- il PdA, che provvede all'inoltro materiale dell'atto informatico e alla ricezione e archiviazione del contenuto dei messaggi di risposta e alla contestuale emissione automatica di un messaggio di *Delivery Status Notification* (DSN);
- il GC, che provvede al deposito dell'atto presso l'UG indicato e, contestualmente, alla trasmissione del messaggio di attestazione temporale dell'evento di deposito;
- l'UG, che provvede alla acquisizione e pre-elaborazione dell'atto.

Le figure che seguono riassumono i flussi logici generati dalla funzione di "deposito atto":

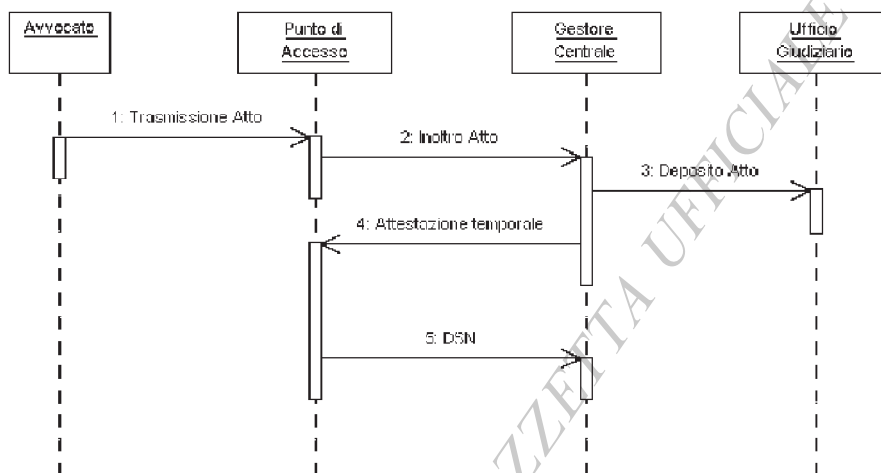



***Figura 4 - Sequence diagram del deposito atto***

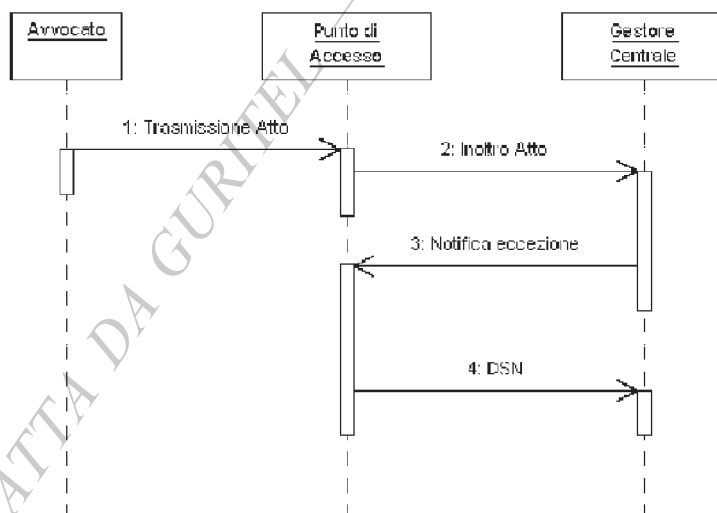



***Figura 5 - Sequence diagram del deposito atto in caso di notifica di eccezione***

### *1.4.2 Ricezione e accettazione dell'atto di parte*

La Figura 6 mostra la sequenza delle operazioni eseguite nella fase di ricezione, da parte dell'UG, dell'atto di parte. Si vogliono qui evidenziare le interazioni di alto livello, le sequenze temporali, il ruolo del registro e del fascicolo informatico.

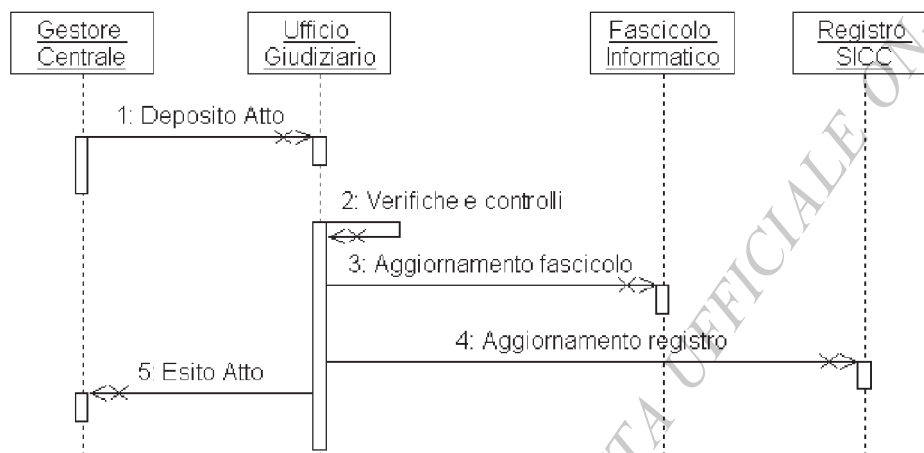



***Figura 6 – Sequence diagram ricezione e accettazione atto di parte***

Descrizione della figura:

1. Il Gestore Centrale invia i contenuti da depositare al sistema informatico dell'ufficio giudiziario.
2. In un istante temporale successivo alla ricezione, l'ufficio giudiziario attiva le procedure di verifica e controllo sui contenuti pervenuti.
3. I contenuti verificati vengono elaborati per l'aggiornamento del fascicolo informatico.
4. In base alle informazioni presenti nell'atto depositato si provvede all'aggiornamento del registro SICC.

A questo punto il deposito effettuato è visibile tramite i servizi di consultazione di Polis Web.

L'Ufficio giudiziario prepara ed invia una comunicazione di esito atto da far pervenire, tramite l'ausilio del Gestore Centrale, all'avvocato mittente.

### *1.4.3 Invio dell'esito di ricezione dell'atto all'Avvocato*

L'invio della notifica di esito dell'atto prevede un flusso di risposta, di direzione opposta a quello del deposito, innescato dalla generazione di un messaggio di esito da parte dell'UG.

Il flusso si completa con il deposito nella casella di posta elettronica di servizio del Punto di Accesso del messaggio di notifica esito. A tale flusso collaborano:

- il GC, che provvede all'inoltro della notifica di esito;
- il PdA, che provvede all'emissione della ricevuta (DSN) per il GC ed a mettere a disposizione dell'Avvocato la notifica di esito.

### *1.4.4 Comunicazioni di cancelleria*

La funzione di invio di un biglietto di cancelleria prevede un flusso di trasmissione di una comunicazione, prodotta dal Cancelliere, alle CPECPT di uno o più Avvocati, e di un flusso di risposta, di direzione opposta, innescato dalla emissione delle singole ricevute di presa in carico delle comunicazioni da parte dei PdA gestori delle CPECPT interessate.

Nella sua interezza il flusso nasce e si completa presso l'UG. A tale flusso collabora:

- il PdA, che genera una ricevuta di presa in carico per ogni messaggio ricevuto, ed una ricevuta breve di avvenuta consegna contestualmente al deposito dello stesso nella CPECPT dell'Avvocato indicato;
- il GC, che provvede all'inoltro delle comunicazioni ai destinatari indicati dall'UG (fase di invio), ed effettua l'attestazione temporale di ogni evento di ricezione di una ricevuta breve di avvenuta consegna da parte dei PdA, per restituirla all'UG mittente (fase di risposta).

Ai fini della valutazione di eventuali termini legali per la consegna della comunicazione, farà fede la data apposta dal GC in fase di attestazione temporale sulla ricevuta breve di avvenuta consegna prodotta dal PdA.

Nella fase 1.0 la funzione sarà limitata nell'invio ad un solo Avvocato. Pertanto, transitoriamente, l'UG dovrà generare tante comunicazioni, una per ogni Avvocato destinatario.

La creazione delle comunicazioni ad opera del cancelliere segue, in questa fase, le stesse modalità attualmente previste dal SICC. Tali comunicazioni, ed in particolare il loro contenuto, sono quindi costruite in maniera automatica dal client SICC evoluto per il processo telematico.

Le evoluzioni vanno nella direzione di gestire quali comunicazioni possono essere inoltrate per via telematica e quali devono essere cartacee mantenendo quindi piena compatibilità con le attuali modalità. Il sistema di cancelleria sarà in grado di gestire in maniera autonoma tali situazioni miste, evitando di chiedere all'utente di cancelleria un intervento manuale per discriminare cosa gestire in cartaceo e cosa in telematico.

La notifica attraverso il sistema del processo telematico prevede quindi che il client SICC crei il contenuto della comunicazione e lo depositi nel sistema di invio dell'UG includendo le informazioni necessarie ad identificare il destinatario (codice fiscale dell'avvocato).

Anche il biglietto di cancelleria, come gli atti di parte, è strutturato secondo il formato XML. La strutturazione data in questa prima fase è tuttavia molto semplice e si limita di fatto ad identificare l'oggetto della comunicazione, il contenuto della stessa e il riferimento al fascicolo di cui fa parte.

Dal punto di vista tecnico il sistema di cancelleria identifica ogni comunicazione con un identificatore univoco che permetterà di legare la comunicazione stessa alla ricevuta di deposito restituita dal GC. Il fascicolo informatico tiene infatti traccia di ogni comunicazione inviata e della relativa ricevuta di consegna.

### *1.4.5 Evoluzione PolisWeb: consultazione web delle informazioni SICC e del fascicolo informatico*

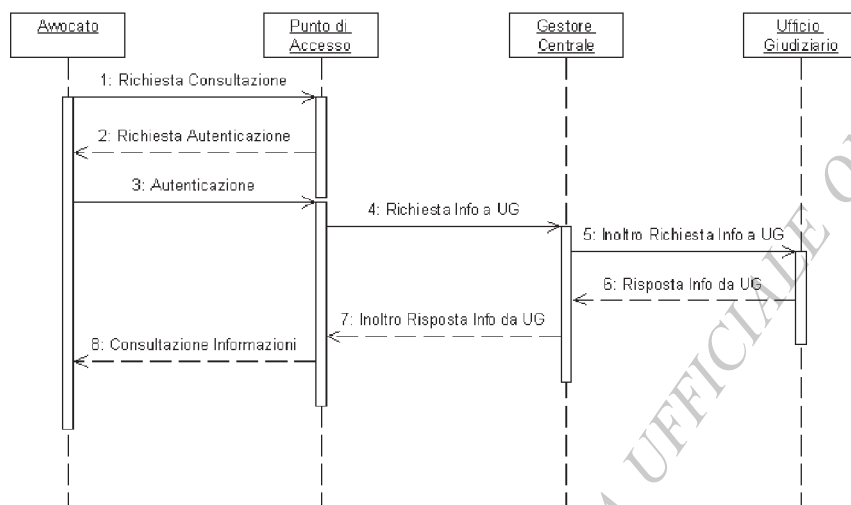



***Figura 7 - Sequence diagram Consultazione Web***

Nella Figura 7 è rappresentato il diagramma di sequenza relativo alla consultazione dei procedimenti personali e degli atti tramite l'applicazione Polis Web fornita sul Punto di accesso. In particolare sono svolte le seguenti azioni:

- L'avvocato sottopone a Polis Web, presente sul PdA, una richiesta di consultazione;
- Il PdA autentica l'utente, se questi non è gia stato precedentemente autenticato, e inoltra la richiesta all'Ufficio Giudiziario, per il tramite del Gestore Centrale;
- Un apposito sottosistema, all'interno dell'UG, predispone le informazioni ottenute a seguito dell'interrogazione del SICC e del sottosistema di gestione del fascicolo informatico (repository documentale) e le inoltra al PdA, per il tramite del GC;
- Polis Web presenta le informazioni in consultazione all'Avvocato.

# 2 DESCRIZIONE DELLE PRINCIPALI FUNZIONALITÀ

*Si precisa che gli strumenti software a disposizione dell'avvocato, descritti in questo capitolo, sono forniti dal Ministero della Giustizia ai soli fini della sperimentazione.*

## *2.1 ATTI DI PARTE COINVOLTI NELLA FASE 1.0*

Di seguito è riportato l'elenco degli atti di parte di cui è possibile la redazione e il deposito in fase 1.0:

| Atto di Citazione |
|---|
| Nota di Iscrizione a Ruolo |
| Atto di citazione in opposizione a d. i. |
| Ricorso per ingiunzione art. 633 cpc |
| Ricorso per ingiunzione artt. 633 e 642 cpc |
| Ricorso per consegna di cose fungibili |
| Ricorso per sequestro giudiziario *ante causam* |
| Ricorso per sequestro conservativo *ante causam* |
| Reclamo avverso provvedimento cautelare |
| Ricorso per separazione |
| Ricorso per divorzio |
| Comparsa di costituzione e risposta |
| Comparsa di costituzione con domanda riconvenzionale |
| Comparsa di costituzione con chiamata di terzo |
| Memoria generica |
| Comparsa ex art. 180 cpc |
| Memoria ex art. 183 |
| Replica ex art. 183 cpc |
| Memoria ex art. 184 |
| Replica ex art. 184 |
| Comparsa conclusionale ex art. 190 |
| Memoria conclusionale di replica ex art. 190 |

Il modello proposto per ciascun atto tiene conto della normativa di riferimento e su di esso è stata studiata una suddivisione strutturale basata sull'analisi dei principali formulari in commercio ulteriormente arricchiti, per i profili informativi in esame, dal lavoro svolto in sede di analisi.

È importante sottolineare che, la linea guida seguita in fase di analisi nella definizione di tali campi, è stata quella di optare comunque per il **carattere opzionale di ogni altro campo e sezione**, liberamente componibile dall'avvocato nella successione argomentativa dallo stesso ritenuta più idonea, qualora la valorizzazione del campo in oggetto non derivi da vincoli imposti dalla logica stati-eventi del sistema SICC, ossia in sostanza non sia necessaria per l'inserimento dell'evento.

La strutturazione dei modelli DTD (Document Type Definition) è pubblicata con apposito decreto ministeriale a parte.

## *2.2 L'AMBIENTE DEL REDATTORE SPERIMENTALE*

L'ambiente di redazione è uno strumento integrato in *Microsoft Word* che consente la predisposizione dell'atto per la successiva trasformazione in formato XML.

Attraverso gli strumenti applicativi disponibili in Word, l'utente redige l'atto, nelle sue parti obbligatorie ed opzionali. Le funzionalità disponibili in fase di redazione, sono attivabili in diversi modi, per esempio attraverso una barra degli strumenti, un menù o abbreviazioni da tastiera.

Le funzionalità native di MS Word sono utilizzate, dove possibile, nell'ambiente di redazione, mentre quelle non consentite sono disabilitate all'utente.

L'ambiente di *editing* è lo stesso di un normale documento Word, e viene proposto all'utente dopo un apposito data-entry per i dati configurati come obbligatori nel modello di atto scelto.

*Si ribadisce che tale obbligatorietà si riferisce ai dati necessari per registrare l'evento SICC.*

Il Sistema, avendo a disposizione un modello ed un documento di default per l'atto che l'utente ha deciso di redigere, presenterà nell'ambiente di redazione un documento con:

- una intestazione contenente tutti i dati definiti come obbligatori nel modello stesso;
- una serie di sezioni (il cui ordine è definito nel modello, ma può essere modificato in fase di data-entry iniziale) riempibili opzionalmente a cura dell'utente Avvocato;
- una formula testuale pre-determinata per ogni sezione, che potrà essere modificata e/o cancellata dall'utente solo sull'Atto stesso senza lasciare parti di testo inconsistenti o righe vuote se non espressamente inserite.

Il Documento Word è, così, organizzato come un insieme gerarchico di Sezioni e Campi, secondo una struttura ad albero: l'intero documento costituisce il Campo radice (root, comune a tutti gli Atti) che può contenere testo e/o Campi figli, e così via, ricorsivamente, esattamente come avviene per i documenti XML. Pertanto ogni parte del Documento appartiene ad un Campo e ogni Campo ne può contenere altri. I Campi del Documento corrispondono biunivocamente ai nodi dell'XML.

Il Sistema permette inoltre all'utente Avvocato di inserire all'interno di ciascuna sezione uno o più campi strutturati (suggeriti dal sistema stesso), e di norma opzionali, la cui compilazione, nel caso di dati complessi, è guidata tramite una finestra di inserimento che controlla l'obbligatorietà o l'opzionalità dei dati stessi contenuti nel campo.

Durante la fase di redazione vera e propria, l'applicativo esercita un costante controllo sull'attività dell'utente al fine di sincronizzare il contesto alla posizione corrente di redazione nel Documento: in ogni istante, lo Strumento di Redazione abilita esclusivamente le funzioni valide nel nodo corrente. Inoltre, impedisce modifiche alla struttura, al fine di garantire la creazione di file XML validi rispetto ai requisiti definiti per il singolo Atto con l'ausilio dei DTD.

L'atto in formato XML, conforme ai DTD previsti dall'Amministrazione, è ottenuto a partire dal formato Word mediante l'esecuzione di procedure specifiche ed automatiche. Il formato dell'Atto XML include, oltre alle marcature "semantiche", ove previsto, anche le informazioni di formattazione del testo.

L'ambiente di redazione così strutturato ha <u>carattere sperimentale</u> e la sua progettazione tiene conto dell'esigenza di apertura verso eventuali indicazioni da parte degli utenti Avvocati che,

durante la sperimentazione, potranno validare le scelte funzionali fatte e contribuire ad un'evoluzione migliorativa dell'applicazione.

La logica progettuale sarà, in ogni caso, "application to application", ossia mira alla realizzazione di un'integrazione tra applicazioni in modo tale da consentire loro di interagire e scambiarsi dati in modo autonomo.

*Si aggiunge infine che la scelta, operata per la fase di sperimentazione, è quella di* ***non introdurre vincoli di alcun tipo*** *all'accettabilità dell'atto, fermo restando le informazioni essenziali che consentono di farlo pervenire all'ufficio giudiziario destinatario.*

## *2.3 CIFRATURA E FIRMA DELL'ATTO DI PARTE*

L'atto redatto sulla postazione client deve essere firmato e cifrato per l'Ufficio Giudiziario di destinazione.

La modalità di apposizione della firma individuata, denominata **firme indipendenti (meccanismo "aggiungi una firma")**, prevede che uno o più soggetti firmano digitalmente lo stesso documento. L'ordine di apposizione delle firme degli N firmatari non è significativo, ed il file generato si presenta con un'unica estensione *p7m*.

La struttura è quindi PKCS#7 in cui sono contenute le N firme che si riferiscono quindi, al medesimo documento. Non è possibile utilizzare tale meccanismo per stabilire l'ordine in cui le firme stesse sono state apposte: una alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica PKCS#7.

Tale meccanismo è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

In Figura 8 è rappresenta la struttura PKCS#7 del file firmato.

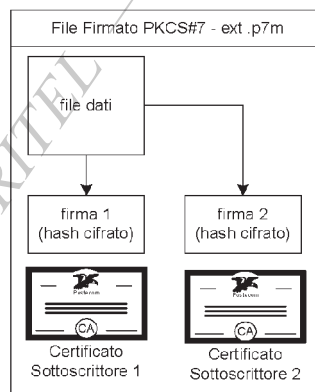



***Figura 8 – Struttura del file firmato***

Per la fase 1.0 del progetto si prevede l'apposizione della firma singola, ovvero effettuata da un unico firmatario.

Tali oggetti, creati sulla postazione dell'avvocato, vengono aggregati, ai fini del deposito, in un'opportuna struttura dati denominata "busta MIME" che contiene le informazioni di

instradamento, i riferimenti ai documenti atto ed allegati, l'atto firmato (*corpoatto.xml.p7m*) e gli eventuali allegati (nella figura che segue l'allegato è *AllegatoX.pdf.p7m*) .

Di seguito viene rappresentata la struttura dell'oggetto MIME, di cui è fornito apposito DTD.

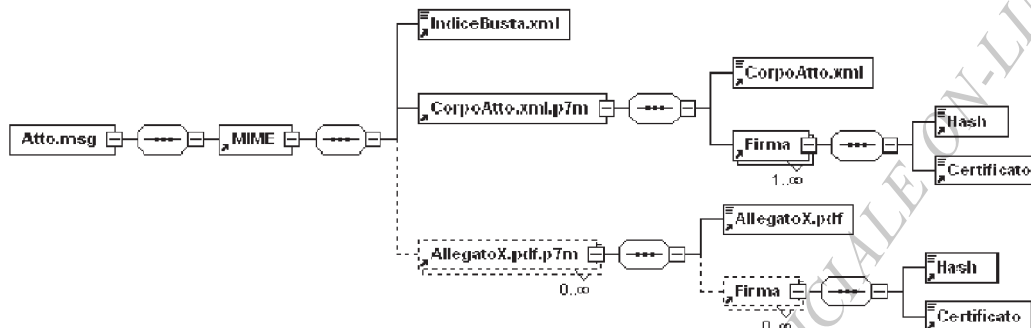



***Figura 9 - Struttura MIME contenente l'atto i suoi allegati e l'indice degli stessi***

La busta così composta è successivamente cifrata per l'ufficio giudiziario di destinazione, in modo che soltanto questo ufficio possa decifrarlo e quindi leggere il contenuto della busta.

Lo standard previsto è il PKCS #7.

"Atto.msg" è l'atto cifrato con chiave di sessione. "ChiaveSessione" è la chiave di sessione cifrata con il certificato del destinatario. "Issuer Dname" è il *Distinguished Name* della CA che ha emesso il certificato dell'ufficio giudiziario destinatario, "*Serial Number*" è il numero seriale del certificato dell'ufficio giudiziario destinatario. Tali dati sono necessari per il controllo successivo in fase di decifratura ed identificano il certificato con cui è stato cifrato l'oggetto.

Di seguito viene rappresentato lo schema della busta ottenuta a seguito del processo di cifratura dell'oggetto mime contenuto nell'oggetto Atto.msg.

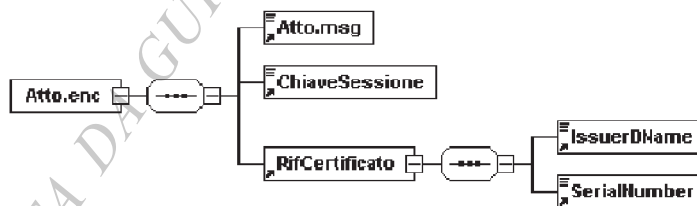



***Figura 10 - Schema del risultato dell'operazione di cifratura di Atto.msg***

L'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione vengono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario con il quale si intende corrispondere.

Tale busta sarà successivamente depositata presso l'Ufficio Giudiziario per il tramite del Punto di Accesso e del Gestore Centrale.

Relativamente alla cifratura degli atti in uscita, ossia cifrati a cura del gestore locale con la chiave pubblica del soggetto abilitato esterno (disponibile sul registro generale degli indirizzi presso il gestore centrale), si applicano le stesse specifiche sopra riportate.

In particolare, per gli atti inviati alla casella di posta certificata del destinatario, verrà utilizzata la medesima struttura di *atto.enc*, che verrà allegato al messaggio di posta elettronica certificata.

Ai fini della consultazione web degli atti, sarà valido quanto segue:

- il GL prepara la risposta SOAP alla richiesta di consultazione e inserisce all'interno di questa un "blob" (in codifica base64) che a sua volta contiene:
  - L'XML dell'atto richiesto, cifrato con crittografia simmetrica utilizzando l'algoritmo 3-DES e chiave di sessione;
  - la chiave di sessione cifrata con la chiave pubblica del certificato di cifratura dell'Avvocato;
  - il certificato utilizzato per la cifratura.
- Il Front-End di Polis Web riceve la risposta SOAP, estrae il "blob" e prepara la risposta HTML inserendo all'interno di essa il "blob".

## *2.4 RICEZIONE E ACCETTAZIONE DELL'ATTO DI PARTE*

Nel presente paragrafo sono analizzate le funzionalità dei componenti tecnologici ad ausilio della cancelleria coinvolti nella fase di ricezione e accettazione dell'atto di parte. In particolare l'attenzione sarà posta sulla gestione delle potenziali situazioni di errore, sia di tipo strettamente tecnico che nel merito del contenuto dell'atto, sull'interfacciamento con il SICC, sulla gestione del fascicolo elettronico e infine sulla modalità con cui la cancelleria comunica all'avvocato mittente l'esito delle operazioni compiute a seguito della ricezione dell'atto.

L'analisi dell'intera infrastruttura dell'UG avrà come necessario punto di partenza la qualità progettata per il SICC che, come richiesto anche dal capitolato tecnico del presente progetto, non dovrà essere in alcun modo intaccata in quanto ha permesso di raggiungere un notevole livello di affidabilità.

Nel momento in cui l'atto viene ricevuto dalla cancelleria l'avvocato mittente ha già ricevuto l'attestazione temporale da parte del GC che ufficializza l'avvenuto deposito dell'atto nel dominio giustizia. E' infatti il GC che funge da "sportello virtuale" per l'avvocato verso il sistema informativo del Processo Civile Telematico.

E' quindi importante distinguere i tre momenti temporali di seguito definiti:

a) **il deposito**, scandito dal GC ed in riferimento al quale è necessario verificare le eventuali scadenze dei termini per il deposito stesso;

b) **la ricezione** da parte dell'UG;

c) **l'accettazione da parte del sistema di cancelleria** a seguito della quale viene scatenato l'evento del SICC e viene concessa visibilità dell'atto, a tutte le parti coinvolte nel procedimento giudiziario, inserendolo nel fascicolo elettronico.

Il ruolo del GC è definito dalle specifiche del presente progetto in sede di capitolato tecnico e quindi la distinzione tra i primi due punti è di fatto obbligata. L'introduzione dell'ultimo asincronismo, tra ricezione e accettazione, si è resa necessaria data la criticità del sistema dei controlli il quale potrebbe introdurre sensibili appesantimenti sul sistema di ricezione se con esso si trovasse a coincidere, con evidenti svantaggi sull'intera infrastruttura.

*Si precisa comunque che i passi "b" e "c" sono di norma eseguiti uno di seguito all'altro, nel giro di qualche istante, a meno che non risulti impossibile scatenare l'evento del SICC.*

Nel seguito si elenca la classificazione degli errori e degli allarmi così come individuata in fase di analisi:

- errore fatale: non è possibile innescare la catena di controlli. Due possibilità:
  - impossibilità di decifrare la busta contenente l'atto e i suoi eventuali allegati assemblati come messaggio MIME multipart;
  - la busta decifrata non è un messaggio MIME multipart.
- errore bloccante: non è possibile scaricare l'evento SICC e l'inserimento nel fascicolo informatico; varie possibilità:
  - IndiceBusta in formato non corretto e quindi non utilizzabile dal sistema.
  - Non è presente l'atto giudiziario.
  - Non è presente un allegato particolare, necessario per eseguire l'evento specifico (es. nota di iscrizione a ruolo nel caso di deposito di un atto di citazione).
  - Atto o allegato non conforme al formato del file richiesto dalle Regole Tecniche, per cui file in formato .pdf, .rtf, .txt, .jpg, .gif, .tiff, .xml, .zip, .rar.
  - Atto o allegato non integro rispetto alla firma elettronica apposta sullo stesso.
  - Il firmatario dell'atto non è costituito parte in causa nel procedimento a cui l'atto si riferisce (nel caso di atti depositati in corso di causa).
  - Il firmatario non è costituito nell'atto introduttivo.
  - Impossibilità di elaborare la struttura dell'atto (errore nel formato XML).
  - Numero di Ruolo non esistente nel SICC o non indicato.
  - Tipologia di atto non previsto.
  - Non completezza o non correttezza dei dati necessari ad innescare l'evento SICC.
  - Altro (eventuali errori che emergeranno dalla fase di sperimentazione)
- allarme: è stato possibile scaricare l'evento SICC ed effettuare l'inserimento nel fascicolo informatico, ma vengono segnalate anomalie nel contenuto dell'atto o nell'insieme degli eventuali allegati; varie possibilità:
  - Il mittente non è il firmatario dell'atto.
  - L'avvocato costituito nell'atto introduttivo non è abilitato. Questo tipo di controllo si rende necessario anche a livello di UG in quanto se il mittente non è il firmatario dell'atto l'abilitazione di quest'ultimo non è stata possibile da parte del PdA o GC in quanto l'atto è cifrato. Le verifiche delle credenziali di un avvocato a livello di UG avviene attraverso la chiamata ad un apposito servizio del GC.
  - Presenza di allegati non indicati nell'indice della busta.
  - Assenza di allegati indicati nell'indice della busta.
  - Atto depositato fuori termine.
  - Data in citazione non possibile (festivo, periodo feriale, fuori dai termini,…).
  - Struttura non conforme ai modelli ovvero ai DTD ministeriali, tipicamente manca una sezione, ad esempio non conformità rispetto alla strutturazione definita dall'articolo 163 per l'atto di citazione.
  - Altro (dipendente dalla strutturazione degli atti ed eventualmente emergente dalla fase di sperimentazione).

- informazione di esito positivo: viene registrato l'esito positivo della fase di controllo e innescato il sistema di accettazione.

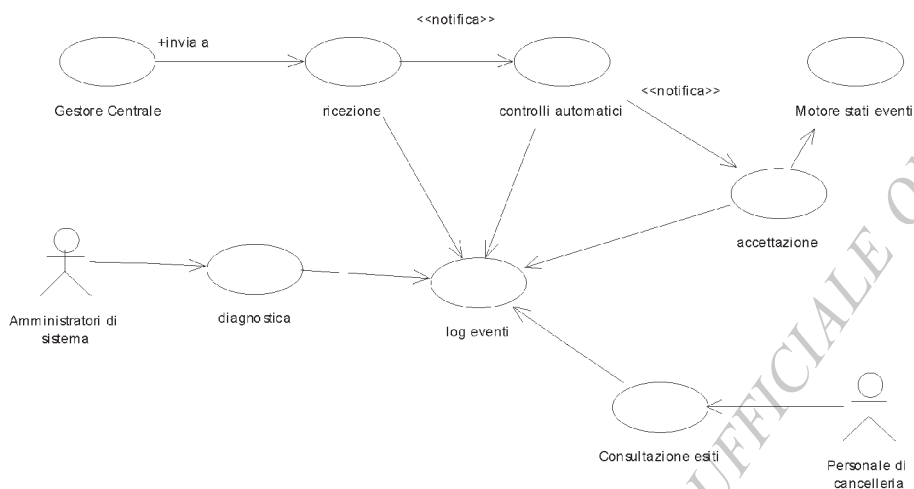



***Figura 11 - Attori e componenti applicative coinvolte in fase di ricezione e accettazione***

*Descrizione della figura:*

Come risulta evidente dalla figura la componente applicativa più importante dell'intero sistema è quella denominata ***Log Eventi***. Il log eventi è un'insieme persistente di informazioni che permettono di tracciare **tutte le operazioni** che, sia le componenti applicative sia gli operatori di cancelleria, effettuano sugli atti in ingresso all'UG. Il documento di analisi architetturale definirà in maniera più esplicita e tecnicamente esaustiva le caratteristiche di questa componente mentre nel contesto del presente documento è sufficiente indicare che viene utilizzata per registrare la tipologia di operazione che il sistema o l'operatore esegue (in forma codificata), la descrizione di tale operazione, il riferimento al documento (atto o allegato) oggetto dell'operazione e l'indicazione temporale del momento in cui viene eseguita.

Nel caso più semplice, ovvero di totale assenza di eccezioni, nel log eventi verrà tenuta traccia delle seguenti operazioni:

- data e ora di ricezione di un atto;
- data e ora dei controlli su di esso effettuati;
- data e ora in cui l'evento del SICC viene scaricato e il fascicolo elettronico aggiornato;
- data e ora di invio della notifica, al mittente, dell'avvenuta accettazione dell'atto da parte della cancelleria.

**Il sistema di ricezione** è l'interfaccia esposta dall'UG verso il GC e si occupa esclusivamente di ricevere attraverso una comunicazione sincrona l'atto giudiziario e i suoi allegati in una busta cifrata con chiave pubblica dell'UG. Il componente si occupa di gestire attraverso meccanismi tipici del protocollo di comunicazione (HTTP) eventuali problemi trasmissione a meno dei quali la busta viene memorizzata localmente in un'area del repository Documentale denominata *Area Buste*. La memorizzazione nell'area buste garantisce sicurezza

dell'avvenuta ricezione di una busta integra in tutte le sue componenti ovvero informazioni sul mittente, attestazione temporale e pacchetto dati cifrato contenente l'atto giudiziario e i suoi eventuali allegati.

**Il sistema dei controlli** è una componente altamente configurabile che permette di individuare eventuali errori bloccanti o semplici anomalie sull'atto depositato e comunicare le stesse all'operatore di cancelleria attraverso il log eventi. Verrà realizzato un vero e proprio sistema di *ruling* altamente personalizzabile con l'obiettivo di conferire al sistema un alto grado di flessibilità ed elasticità necessario soprattutto nella fase sperimentazione.

**Il sistema di accettazione** è in grado di utilizzare il motore stati eventi per lo scarico dell'evento corrispondente al deposito dell'atto e di memorizzare l'atto stesso nel fascicolo elettronico attraverso l'interfacciamento con il repository documentale. Il sistema di accettazione viene attivato solo nel caso in cui tutti i controlli diano esito positivo.

**Il motore stati eventi** è esattamente lo stesso che viene attualmente utilizzato dal SICC.

**Il fascicolo elettronico indica** quell'area del repository documentale utilizzata per la memorizzazione degli atti di parte e d'ufficio e dei relativi allegati.

**Il sistema di diagnostica** è utilizzato dagli amministratori di sistema dell'UG per individuare e intervenire a livello esclusivamente tecnico sull'atto pervenuto all'UG. Il sistema di diagnostica fornisce agli amministratori un'interfaccia attraverso la quale registrate gli interventi nel log eventi.

**Il sistema per la consultazione del log eventi** mette a disposizione degli operatori di cancelleria un'interfaccia grafica potente e flessibile che permette loro di verificare tutte le operazioni effettuate dal sistema in automatico. Nel caso di errori o anomalie tale interfaccia permetterà in maniera semplice di intervenire manualmente, laddove possibile, per riuscire comunque ad aggiornare il SICC e il fascicolo elettronico.

### *2.5 Il Fascicolo Informatico*

Il Repository Documentale nasce per gestire il fascicolo informatico, conservare i documenti prodotti nell'ambito di un procedimento giudiziario ed esporre ai sistemi utilizzatori servizi informatici di alimentazione e fruizione delle informazioni. Tale servizio si configura come una piattaforma di gestione documentale che mette in comunicazione i diversi applicativi con la base dati documentale, per consentire l'interazione documentale ed informativa fra soggetti appartenenti a categorie diverse tra loro (Giudice, Cancelliere, Avvocato, CTU).

L'obiettivo principale del Repository Documentale è quello di potenziare le funzionalità delle Applicazioni di Gestione dei Registri, con capacità di Gestione Documentale ed *Information Retrieval* (queste ultime verranno introdotte nella fase 2 del progetto).

In questo modo il Repository Documentale funge da gestore centralizzato del patrimonio documentale, divenendo l'unità di archiviazione univoca e centrale a livello di UG dei documenti prodotti o ricevuti dall'Ufficio stesso, indipendentemente dalla loro natura originaria, analogica o digitale.

Nella fase sperimentale del Processo Telematico, il Repository Documentale esporrà un insieme limitato di servizi; sarà infatti compito del SICC, in questa prima fase, ricevere le richieste di accesso al patrimonio documentale, filtrarle sulla base dei criteri di visibilità insiti nelle proprie strutture dati e formulare specifiche richieste al Repository Documentale.

Il SICC, in questa fase, sarà il sistema tenutario di tutte le informazioni che riguardano la vita del Fascicolo; il Fascicolo Informatico gestito in ambito del Repository Documentale pertanto sarà limitato alla memorizzazione dei Documenti depositati da soggetti esterni ed interni all'Ufficio Giudiziario, provvedendo a mantenere il legame con il Procedimento corrispondente sul SICC.

Riguardo ai Documenti informatici, il legame tra SICC e Repository verrà assicurato attraverso l'implementazione della relazione Eventi – Atti, che associa a ciascun Evento che accade ad un Procedimento sul SICC il/i Documenti che lo hanno generato, memorizzati sul Repository. In questa prima fase progettuale il Repository Documentale, pertanto, si limiterà ad esporre le seguenti categorie di servizi:

- acquisizione dei documenti contenuti nelle Buste ricevute dal Gestore Centrale, confezionate allo scopo di depositare gli Atti, dagli Avvocati che partecipano alla fase sperimentale del progetto;
- acquisizione delle comunicazioni inviate dalla Cancelleria dell'Ufficio Giudiziario verso l'esterno, quali ad esempio i Biglietti di Cancelleria;
- consultazione di documenti.

A titolo esemplificativo, il seguente diagramma di sequenza illustra le modalità di interazione tra SICC e Repository Documentale nella fase sperimentale del Processo Telematico, relativamente alle richieste di consultazione documenti inoltrare da PolisWeb.

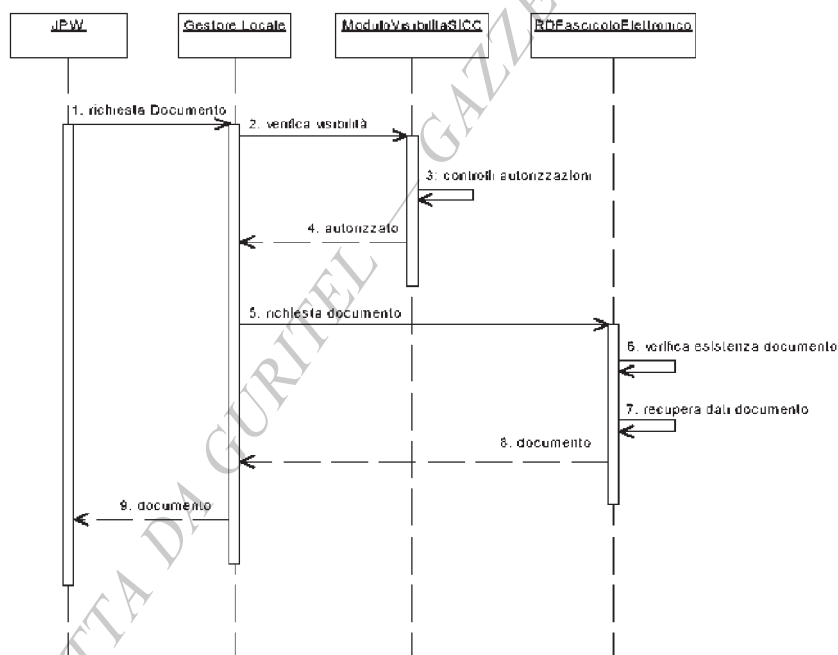



***Figura 12 – Diagramma di sequenza "Interazioni SICC – repository documentale"***

<u>Spiegazione</u>:

1. Il Sottosistema Polis Web (JPW) inoltra una richiesta di visualizzazione Documento;

2. Il Gestore Locale invia la richiesta di verifica dei diritti di visibilità al Modulo Visibilità del SICC;
3. Il SICC effettua i controlli sui diritti di visibilità inerenti la richiesta;
4. Il SICC restituisce al Gestore Locale l'informazione relativa alla presenza o assenza dell'autorizzazione;
5. A seguito dell'autorizzazione da parte del SICC, il Gestore Locale richiede il Documento al Repository Documentale;
6. Il Repository Documentale verifica l'esistenza del Documento;
7. Il Repository, trovato il documento, provvede a recuperarlo;
8. Il Repository invia il documento richiesto al Gestore Locale;
9. Il Gestore Locale invia il documento al Sottosistema JPW che ne aveva richiesto la visualizzazione.

**Gli ambienti del Repository Documentale**

Gli ambienti nei quali il Repository Documentale è suddiviso nella fase sperimentale del Progetto sono i seguenti:

*Ambiente di Memorizzazione delle Buste*; tale ambiente è demandato alla memorizzazione e conservazione delle Buste inoltrate dal Gestore Centrale all'Ufficio Giudiziario e, viceversa, delle Buste inoltrate dall'Ufficio Giudiziario al Gestore Centrale, le quali vengono conservate localmente per essere successivamente elaborate dalla componente di controllo (cfr. 2.4).

*Ambiente di Pre-Accettazione*; in questo ambiente sono memorizzati, in maniera temporanea, i documenti contenuti in ciascuna Busta scambiata con il Gestore Centrale; tali documenti verranno successivamente recepiti ai fini della accettazione dei Documenti in ingresso.

*Ambiente Fascicolo Elettronico*; contiene i documenti elettronici ricevuti dal Gestore Centrale e sottoposti al processo di accettazione da parte del SICC ed i documenti prodotti all'interno dell'Ufficio Giudiziario ed inoltrati al Gestore Centrale; tali documenti rappresentano gli Atti dei Procedimenti Giudiziari e sono raccolti in fascicoli, ricalcando le logiche applicative che legano un Procedimento Giudiziario al relativo fascicolo cartaceo.

## 2.6 COMUNICAZIONI DI CANCELLERIA

Allo stato attuale il SICC gestisce le comunicazioni in forma cartacea ed in particolare a seguito di un aggiornamento del fascicolo e quindi dello scarico di un evento viene proposto al cancelliere di stampare le comunicazioni, una per ogni parte, più un report riassuntivo da inserire nel fascicolo d'ufficio.

L'emissione del biglietto di cancelleria non è vincolata allo scarico di un evento e il suo contenuto può essere esplicitamente scritto dal cancelliere, è per questo che si è definita nel SICC la tipologia *comunicazione generica*.

A seguito della consegna al destinatario viene da questi rilasciata la ricevuta breve di avvenuta consegna che sarà anch'essa inserita nel fascicolo d'ufficio.

Viene di seguito riportato l'elenco delle comunicazioni di cancelleria considerate in questa fase di analisi:

- Nomina Giudice
- Sostituzione Giudice
- Fissazione data udienza
- Sostituzione sezione
- Nomina CTU
- Convocazione CTU
- Revoca CTU
- Liquidazione CTU
- Nomina o revoca di Tutore/Curatore
- Avviso di deposito sentenza
- Comunicazione generica

La funzione di invio di un biglietto di cancelleria prevede un flusso di trasmissione dall'UG verso le caselle di posta elettronica del processo telematico di tutti gli avvocati coinvolti nel procedimento giudiziario a cui la comunicazione è riferita. In seguito al deposito su tale casella di posta viene attivato il flusso di risposta, innescato dalla emissione delle singole ricevute di avvenuta consegna da parte dei PdA gestore delle caselle di posta interessate.

Nella sua interezza il flusso nasce e si completa presso l'UG e a tale flusso collabora:

- il GC, che provvede all'inoltro delle comunicazioni ai destinatari indicati dall'UG (fase di invio), ed effettua l'attestazione temporale di ogni evento di ricezione di una ricevuta di avvenuta consegna da parte dei PdA, per restituirla all'UG mittente (fase di risposta).

- il PdA, che genera una ricevuta di presa in carico per ogni messaggio ricevuto ed una ricevuta di avvenuta consegna contestualmente al deposito dello stesso nella CPECPT dell'avvocato indicato;

Ai fini della valutazione di eventuali termini legali per la consegna della comunicazione farà fede la data apposta dal GC, in fase di attestazione temporale, sulla ricevuta di avvenuta consegna prodotta dal PdA.

## *2.7 Consultazione Web (Jpw)*

Il sottosistema PolisWeb fornisce strumenti per la consultazione via Web delle informazioni contenute nei Registri dei Procedimenti e/o nei Documenti afferenti ad un Procedimento (Fascicolo Elettronico) o alla Base Dati Giurisprudenziale dei Provvedimenti pubblicati.

L'attuale sistema PolisWeb fornisce una serie di servizi informativi riguardanti sia la giurisprudenza che la gestione operativa dei fascicoli e delle udienze del Contenzioso Civile relative ad ogni singolo Ufficio Giudiziario.

L'applicazione PolisWeb è rivolta a ***tipologie di utenti*** distinti in base al proprio ruolo, identificabili come Utente di Consultazione, Utente di Cancelleria e Utente di Amministrazione.

- L'Utente di Consultazione è genericamente un Avvocato, abilitato all'utilizzo dell'applicazione da un Utente di Amministrazione dell'Ufficio Giudiziario. Il sistema PolisWeb è utilizzabile dall'Avvocato sia all'interno dell'Ufficio Giudiziario, tramite

delle postazioni di lavoro dedicate e definite “Chiosco” (Intranet), che dal proprio Studio Legale attraverso il proprio browser web con collegamento Internet.

- L’Utente di Cancelleria è un operatore di cancelleria che attraverso PolisWeb è in grado di utilizzare le funzionalità relative alla gestione delle richieste di copie di documenti effettuate dall’Avvocato tramite le specifiche funzioni messe a disposizione da PolisWeb.
- L’Utente di Amministrazione gestisce le richieste di Account e le relative attivazioni e abilitazioni per gli Utenti di Consultazione e di Cancelleria.

PolisWeb, potrà essere installato e configurato all'interno dell'UG, allo scopo di rispondere alle richieste informative provenienti dai cosiddetti "chioschi" presenti nelle sale degli UG (***Modalità Intranet***) e, allo stesso modo, essere installato su server esterni al confine del Sistema Informativo Civile, quali ad esempio i Punti di Accesso. In tale caso PolisWeb sarà capace di sfruttare i servizi offerti dagli Uffici Giudiziari attraverso il Punto di accesso ed il Gestore Centrale (***Modalità Internet***).

PolisWeb può quindi essere utilizzato all'interno dell'UG attraverso appositi "chioschi" informativi mentre dall'esterno attraverso i Punti di Accesso.

Di seguito viene rappresentato il diagramma di sequenza relativo alla autenticazione dell’utente al Punto di Accesso:

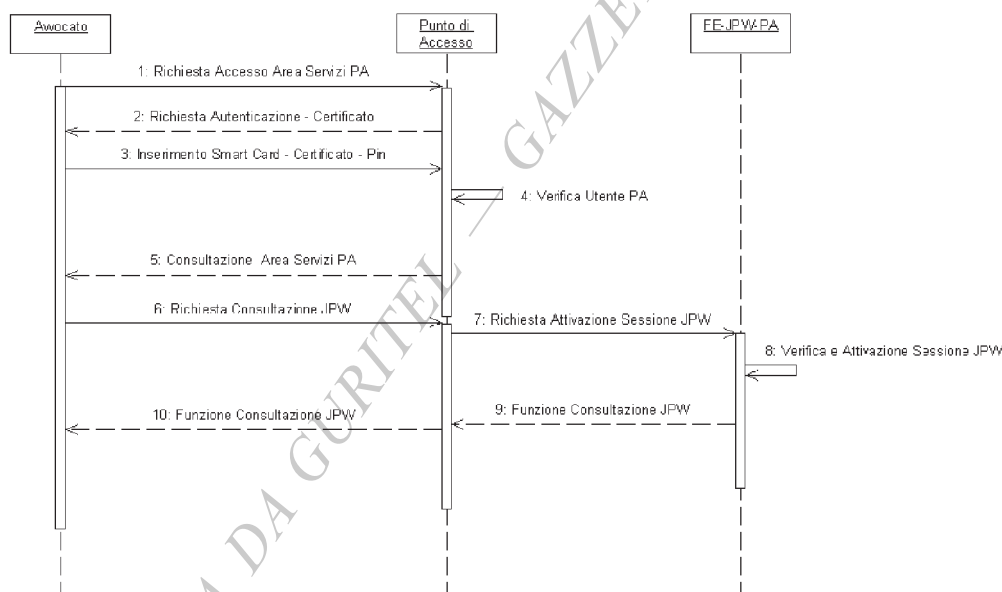



***Figura 13- Flusso Autenticazione PolisWeb da internet***

<u>*Descrizione della figura:*</u>

- La funzione prevede la richiesta da parte di un utente Avvocato di accedere ai servizi web forniti dal Punto di Accesso.

- Per l'accesso all'Area Servizi del Punto di Accesso all'Avvocato viene richiesto il Certificato di Autenticazione.
- L'Avvocato, utilizzando la propria Smart-Card, fornisce al Punto di Accesso il proprio certificato di autenticazione.
- Il Punto di Accesso verifica le informazioni di autenticazione fornite dall'utente Avvocato. La Verifica Utente accerta l'utente come appartenente agli utenti del Punto di Accesso e successivamente la validità del Certificato di Autenticazione ricevuto.
- L'utente Avvocato, a seguito della corretta autenticazione, accede all'area di consultazione dei servizi del Punto di Accesso.
- Dall'area dei servizi del Punto di Accesso l'Avvocato può richiedere l'accesso alle funzioni di consultazione di PolisWeb, installato presso il Punto di Accesso.
- Il Punto di Accesso, a seguito della richiesta dell'Avvocato di accedere alle funzioni di consultazione di PolisWeb, si l'interfaccia con il Front-End di PolisWeb per la richiesta attivazione della sessione utente.
- PolisWeb abilita la nuova sessione utente per l'accesso all'area riservata di PolisWeb, attraverso le informazioni fornite dal Punto di Accesso
- PolisWeb a seguito dell'attivazione della sessione utente, fornisce e permette al Punto di Accesso di presentare all'utente Avvocato la funzione di consultazione di default dell'area privata di PolisWeb.

Nella Figura 14 viene rappresentato il diagramma di sequenza relativo alla consultazione dei procedimenti personali in ambito SICC, attivabili a seguito dell'autenticazione al PdA.

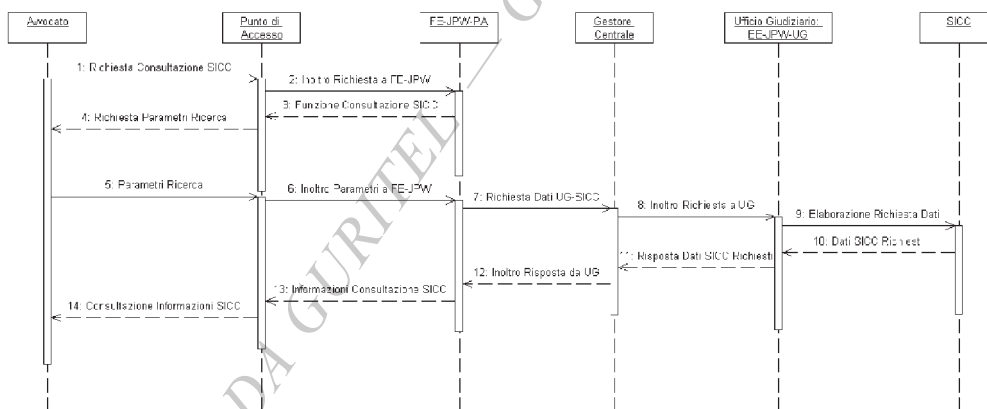



***Figura 14- Flusso Consultazione PolisWeb Internet***

<u>*Descrizione della figura:*</u>

- A seguito dell'autenticazione presso il Punto di Accesso un utente Avvocato può effettuare la richiesta di una funzione di consultazione fornita dal Punto di Accesso attraverso l'integrazione con il PolisWeb installato presso il Punto di Accesso stesso.
- La richiesta dell'Avvocato, di attivazione di una funzione di consultazione, viene inoltrata al Front-End di PolisWeb. PolisWeb fornisce la funzione richiesta per consentire all'Avvocato di indicare i parametri necessari alla ricerca delle informazioni a lui utili.
- I parametri di ricerca forniti dall'Avvocato possono essere ad esempio relativi ad una ricerca di consultazione di informazioni del SICC, fornite da un Ufficio Giudiziario specifico. I parametri sono inoltrati dal Punto di Accesso al Front-End di PolisWeb.
- Il Front-End di PolisWeb, in base ai parametri ricevuti, prepara il messaggio di richiesta (XML-Soap) da indirizzare al Gestore Centrale per l'inoltro all'Ufficio Giudiziario indicato dall'Avvocato.
- La richiesta di informazioni ricevuta dal Back-End di PolisWeb presso l'Ufficio Giudiziario (Servzi Soap dell'Application Server Comune) viene elaborata con l'interrogazione della base dati di interesse (SICC e/o Fascicolo Elettronico).
- Le informazione così individuate, sono fornite in risposta al Gestore Centrale per l'inoltro al Front-End di PolisWeb presso il Punto di Accesso richiedente.
- L'Utente Avvocato può consultare le informazioni di risposta, in base ai parametri di ricerca precedentemente forniti.

# 3 FLUSSO DI DETTAGLIO PER IL DEPOSITO DI UN ATTO

Il deposito di un atto prevede un flusso di trasmissione dell'atto informatico da un PdA, fino al GL destinatario, e un flusso di risposta, di direzione opposta, innescato dalla produzione di un messaggio di *esito atto*, automatico o su azione del Cancelliere, indirizzato al PdA mittente.

In fase di trasmissione dell'atto è inoltre prevista una risposta al momento della ricezione della richiesta di inoltro dell'atto, da parte del GC. Detta risposta, indirizzata al PdA mittente, consiste nella *attestazione temporale* dell'evento di ricezione e la sua data di emissione avrà valore legale per la verifica dei termini di scadenza per la presentazione dell'atto, salvo verifica di buon fine dell'atto medesimo presso l'UG (verifica delle condizioni minime di accettabilità dell'atto).

Si ricorda che il flusso di deposito atto è originato dall'attivazione da parte di un Avvocato di un apposito servizio offerto dal proprio PdA, e che è sempre compito del PdA presentare all'Avvocato i messaggi di risposta ricevuti dal SIC.

Inoltre per completezza delle casistiche che la funzione in oggetto può generare è necessario prendere in considerazione la possibilità, seppure remota e imputabile ad un errore software, che la busta inoltrata dal PdA possa contenere un errore o una anomalia che impedisce l'inoltro dell'atto al GL. In questo caso il GC genera e invia al PdA un messaggio di *notifica eccezione*. Sarà cura del PdA rimuovere l'errore che ha prodotto la non conformità della busta e provvedere ad una nuova trasmissione.

I messaggi SMTP relativi alla funzione di *deposito atto* vengono ricevuti dal GC all'indirizzo **gestorecentrale@processotelematico.giustizia.it** e spediti al PdA all'indirizzo **<codicePdA>@processotelematico.<dominioPdA>**.

Tali messaggi sono:

- il messaggio di inoltro atto trasmesso dal PdA al GC, contenente Atto.enc e InfoInoltro.xml;
- il messaggio contenente l'attestazione temporale inviato dal GC al PdA (vedi paragrafo 3.1.3);
- il messaggio di notifica eccezione inviato dal GC al PdA alternativo all'attestazione temporale (vedi paragrafo 3.1.4);
- il messaggio di esito deposito inviato dal GC al PdA contenente l'esito del deposito lato UG (vedi paragrafo 3.2.2).

I messaggi ricevuti dal GC hanno una testata SMTP standard in cui viene richiesto di impostare almeno i parametri "MSG-ID" e "FROM" (da utilizzare per individuare la provenienza del messaggio quando non è possibile procedere all'apertura della busta ricevuta).

I messagi inviati dal GC al PdA hanno una testata SMTP standard in cui il subject, in base al tipo di messaggio, ha uno dei seguenti valori: esito atto, attestazione, notifica eccezione.

Al PdA viene anche richiesto di implementare il servizio SMTP standard di Delivery Status Notification (DSN), che assume il valore di ricevuta *debole* dei messaggi di risposta trasmessi dal SIC. La ricezione del DSN da parte del GC consente di controllare il corretto completamento del flusso logico della funzione.

### *3.1 FASE DI TRASMISSIONE DELL'ATTO*

Come anticipato precedentemente la sequenza dei messaggi scambiati tra PdA e GC nella fase di trasmissione dell'atto può dare luogo a diverse alternative in funzione dell'esito dei controlli operati dal GC.

Nel caso in cui il messaggio di inoltro atto ricevuto dal PdA sia corretto la sequenza e il tipo di messaggi scambiati è indicata nello schema seguente:

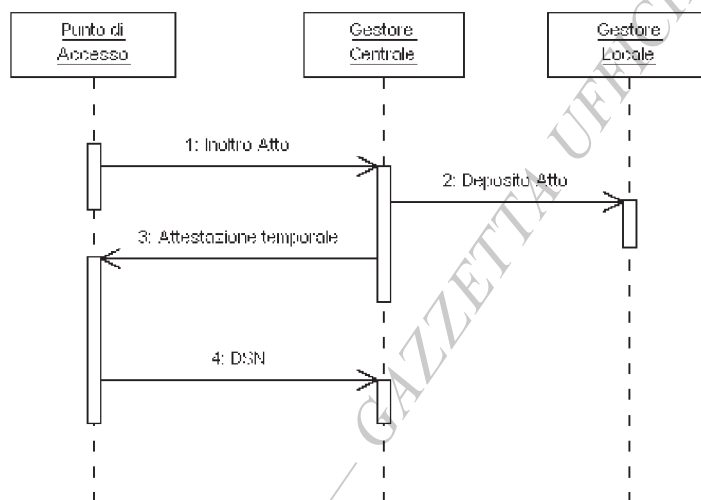



***Figura 15 – Sequence diagram del deposito atto – Fase di trasmissione dell'atto***

Nel caso in cui il GC riscontri un errore nel messaggio di inoltro dell'atto, oltre a non procedere al deposito presso il GL invia al PdA un messaggio di notifica eccezione:

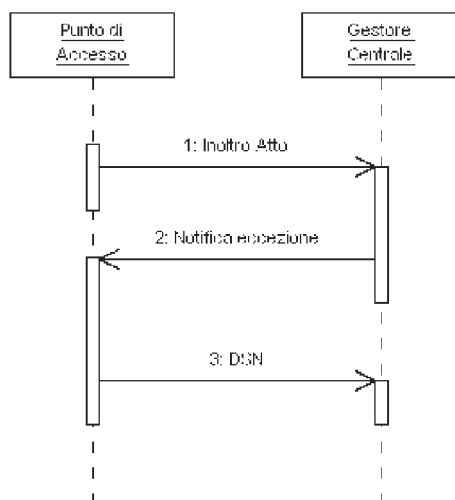



***Figura 16 - Sequence diagram del deposito atto in caso di notifica di eccezione***

Il GC svolge quindi una funzione di garante del processo di inoltro assicurando che gli atti informatici depositati presso i GL non contengano errori attribuibili alle attività svolte dai PdA, ma solo eventualmente ascrivibili ad operazioni svolte in locale dall'Avvocato in fase di formazione dell'atto informatico.

Nel seguito viene descritta la struttura applicativa di ciascun messaggio generato nella fase di trasmissione dell'atto e in allegato vengono forniti i DTD di ciascuna struttura XML utilizzata.

### *3.1.1 Struttura del messaggio di "inoltro atto"*

La struttura del messaggio SMTP di *inoltro atto* proveniente da un PdA è illustrata nella figura che segue:

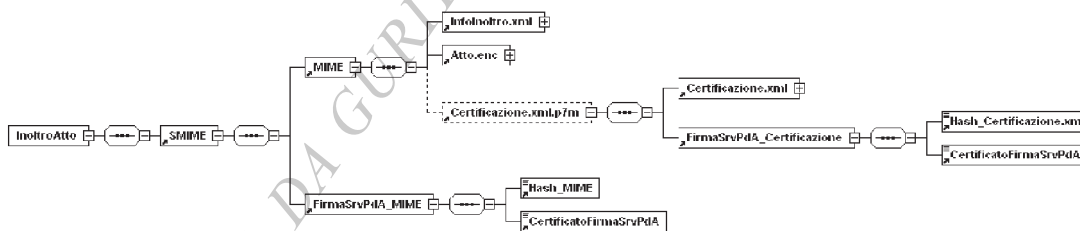



***Figura 17 - S/MIME di Inoltro Atto***

Essa è costituita da un S/MIME, cioè da una struttura MIME sottoscritta da parte del PdA con proprio certificato server, a titolo di verifica della integrità del messaggio.

Pertanto al suo interno è riconoscibile:

- una struttura MIME;

- ♦ l'hash del MIME, cioè la registrazione in formato binario che contiene l'*impronta* del documento, firmata secondo le modalità tecniche previste dal D.P.R. 513/97 e dalle relative regole tecniche (D.P.C.M. 8/02/99).
- ♦ il Certificato del PdA, ossia una struttura dati tipo X.509. I dati forniscono informazioni sul possessore del certificato, il firmatario del certificato, la versione, il numero seriale, l'algoritmo di firma, il periodo di validità, la corrispondente chiave pubblica e altri dati.

Le parti costituenti la struttura MIME sono appresso descritte.

**1. File InfoInoltro.xml**

Il file *InfoInoltro.xml* contiene le informazioni di servizio per il GC. Tali informazioni consentono il routing del messaggio e la verifica dei dati di certificazione.

Il file ha la seguente struttura:

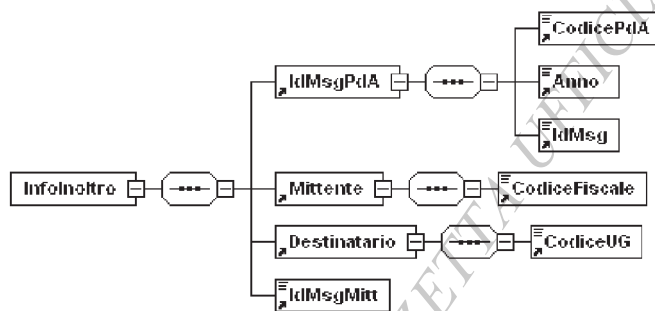



***Figura 18 – Struttura del file InfoInoltro.xml***

- IdMsgPdA.
  Riporta l'identificativo univoco del messaggio generato dal PdA. Tali dati sono:

  *CodicePdA* = E' il codice identificativo del PdA.

  *Anno* = E' l'anno di generazione del messaggio.

  *IdMsg* = E' un progressivo numerico univo nell'ambito dell'anno.

- Mittente.

  *CodiceFiscale* = È il codice fiscale dell'Avvocato che ha originato il messaggio.
  L'attributo *ruolo* indica il ruolo assunto dal mittente (al momento "Avvocato").

- Destinatario.

  *CodiceUG* = È il codice identificativo dell'UG destinatario.
  L'attributo *tipo* indica il tipo di destinatario (al momento "Ufficio"). Al momento è previsto un solo destinatario.

- IdMsgMitt.

  *IdMsgMitt* = È l'identificato assegnato dall'Avvocato all'atto informatico.

**2. File Atto.enc**

Il file Atto.enc è l'atto informatico prodotto dall'Avvocato, criptato utilizzando la chiave pubblica di cifratura dell'UG destinatario.

**3. File Certificazione.xml.p7m**

Il file Certificazione.xml.p7m può mancare nella busta di inoltro atto se il PdA non dispone delle informazioni atte a certificare l'Avvocato.

Se presente tale file è firmato dal PdA (firma server) ed ha la seguente struttura:

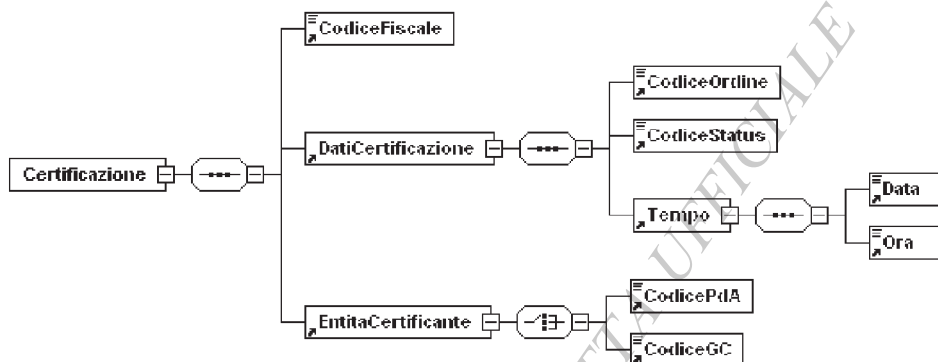



***Figura 19 - Struttura del file Certificazione.xml***

- CodiceFiscale.

  *CodiceFiscale* = È il codice fiscale dell'Avvocato che si certifica (deve coincidere con *InfoInoltro/Mittente/CodiceFiscale*).

- DatiCertificazione.

  Riporta i dati risultanti nell'albo elettronico all'atto della certificazione

  *CodiceOrdine* = E' l'organizzazione (CdO) che ha fornito i dati per la certificazione dello status dell'Avvocato.

  *CodiceStatus* = E' il codice dello status professionale dell'Avvocato risultante all'atto della certificazione (attivo, sospeso, radiato).

  *Tempo* = E' la data e ora in cui viene eseguita la certificazione.

- EntitaCertificante.

  *EntitaCertificante* = È il codice dell'entità che ha eseguito la certificazione (PdA o GC).

### *3.1.2 Struttura del messaggio di "deposito atto"*

La busta di *Deposito atto* presenta la struttura appresso schematizzata:

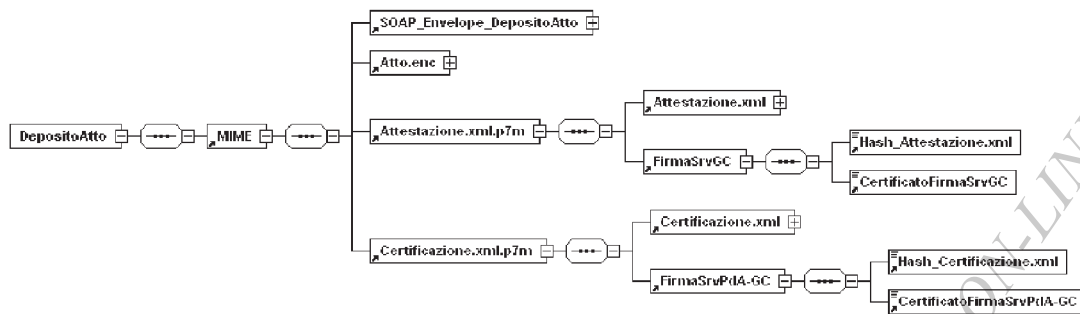



***Figura 20 – MIME di Deposito Atto***

dove la struttura SOAP_Envelope_DepositoAtto ha la seguente rappresentazione grafica:

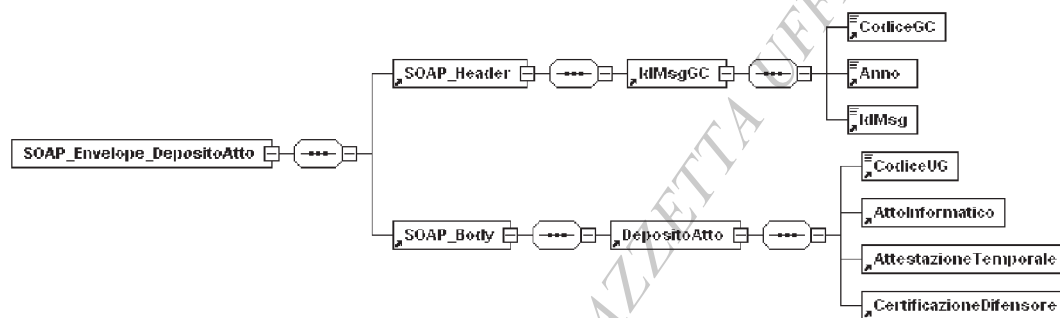



***Figura 21 – Struttura SOAP_Envelope di DepositoAtto***

Il messaggio viene spedito dal GC all'indirizzo identificato dalla URI http://<codiceGL>.processotelematico.giustizia.it/<servizioDepositoAtto>.

La busta *DepositoAtto* contiene le seguenti strutture:

1. **SOAP:Envelope**
   La struttura contiene a livello di header il codice univoco generato dal GC per identificare il messaggio ricevuto (in questo caso il messaggio di *Inoltro atto*).

   Il body della struttura ha un elemento, denominato *DepositoAtto* contenente:

| | | |
|---|---|---|
| *CodiceUG* | = | E' il codice dell'UG cui è destinato l'Atto informatico, ricavato da *InfoInoltro/Destinatario/CodiceUG* |
| *Atto* | = | Referenzia l'Atto informatico (file Atto.enc), generato dall'Avvocato, allegato nel MIME. |
| *AttestazioneTemporale* | = | Referenzia il file Attestazione.xml.p7m, generato e firmato dal GC, allegato nel MIME. |
| *CertificazioneDifensore* | = | Referenzia il file Certificazione.xml.p7m, ricevuto dal PdA o generato e firmato dal GC, allegato nel MIME. |

**2. File Atto.enc**

Si veda il paragrafo 3.1.1.

**3. File Attestazione.xml.p7m**

All'atto della ricezione di un messaggio di *Inoltro atto* da parte del PdA, e dopo averne verificato la correttezza, il GC esegue l'attestazione temporale dell'evento di ricezione della richiesta di inoltro dell'atto.

L'attestazione temporale si sostanzia nella generazione del file *Attestazione.xml*, la cui struttura viene illustrata nella figura che segue:

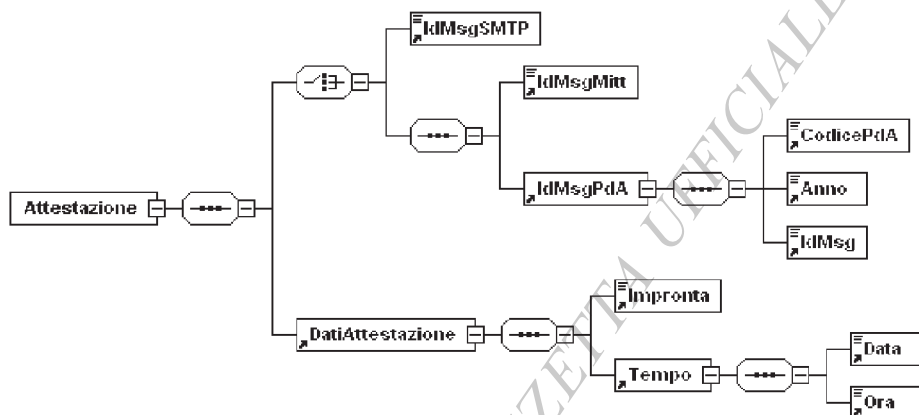



***Figura 22 - Struttura del file Attestazione.xml***

- IdMsgSMTP.

  In questo caso non è valorizzato (tale elemento è alternativo rispetto a i due successivi).

- IdMsgMitt.

  *IdMsgMitt* = È l'identificativo assegnato dall'Avvocato all'atto informatico (ricavato da *InfoInoltro/IdMsgMitt*)

- IdMsgPdA.

  *IdMsgPdA* = È l'identificato del messaggio generato dal PdA (ricavato da *InfoInoltro/IdMsgPdA*)

- DatiAttestazione.

  *DatiAttestazione* = Contiene l'impronta della busta ricevuta (nel formato S/MIME) e la data e ora dell'evento di attestazione temporale

**4. File Certificazione.xml.p7m**

Il file Certificazione.xml.p7m è lo stesso presente nella busta di Inoltro atto (si veda **Figura 19**). Qualora tuttavia il PdA non disponesse delle informazioni atte a certificare l'Avvocato, il GC deve eseguire la certificazione sostitutiva e sottoscrivere il file con la propria firma digitale (firma server).

### *3.1.3 Il messaggio di risposta "attestazione temporale"*

Oltre al deposito dell'atto presso il GL destinatario, il GC genera e trasmette al PdA da cui ha ricevuto la richiesta di inoltro dell'atto, un messaggio di *Attestazione temporale*.

Il messaggio contiene allegato all'interno della struttura MIME lo stesso file Attestazione.xml.p7m trasmesso all'UG.

***Figura 23 – MIME di Attestazione temporale***

### *3.1.4 Il messaggio di risposta "notifica eccezione"*

Qualora il GC riscontri un errore nella formazione della busta di *inoltro atto*, oltre a non eseguire il deposito dell'atto, genera e trasmette al PdA da cui ha ricevuto la richiesta di inoltro dell'atto un messaggio di *Notifica eccezione*.

Il messaggio ha la seguente struttura:

***Figura 24 – MIME di Notifica eccezione***

All'interno della struttura MIME è presente in allegato il file *Eccezione.xml* che ha la seguente struttura:

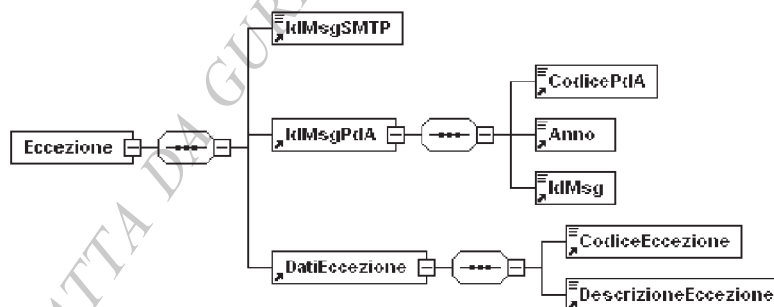



***Figura 25 - Struttura del file Eccezione.xml***

- IdMsgSMTP.

| | | |
|---|---|---|
| *IdMsgSMTP* | = | È l'identificativo SMTP del messaggio ricevuto (parametro Message-ID). Tale identificativo potrebbe costituire l'unico modo di identificare il messaggio, qualora non fosse possibile eseguirne lo sbustamento. |

- IdMsgPdA.

| | | |
|---|---|---|
| *IdMsgPdA* | = | È l'identificativo del messaggio generato dal PdA (si veda il paragrafo 3.1.1). |

- DatiEccezione.

| | | |
|---|---|---|
| *CodiceEccezione* | = | È il codice identificativo dell'errore riscontrato. |
| *DescrizioneEccezione* | = | È la descrizione dell'errore riscontrato. |

## 3.2 FASE DI TRASMISSIONE DELL'ESITO DELL'ATTO

La sequenza e il tipo di messaggi scambiati in fase di trasmissione dell'esito dell'atto è indicata nello schema seguente:

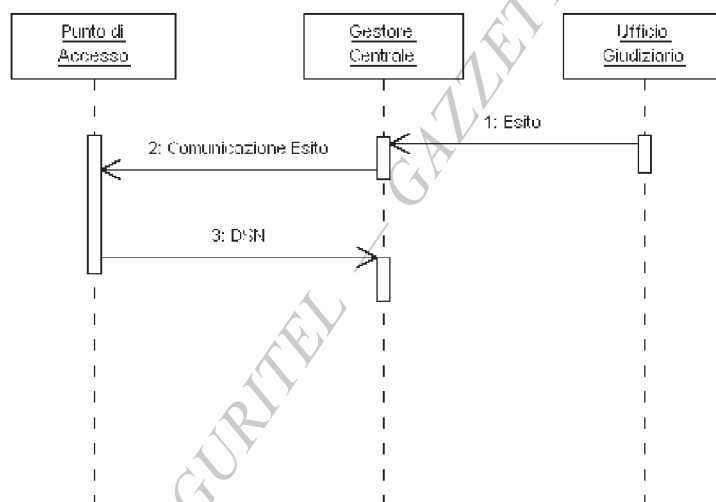



**Figura 26 – Sequence diagram del deposito atto – Fase di trasmissione dell'esito dell'atto**

### 3.2.1 Struttura del messaggio di esito atto

Il GL, in risposta alla ricezione di un atto informatico genera e inoltra al GC un messaggio di *Esito atto* che presenta la struttura appresso schematizzata:

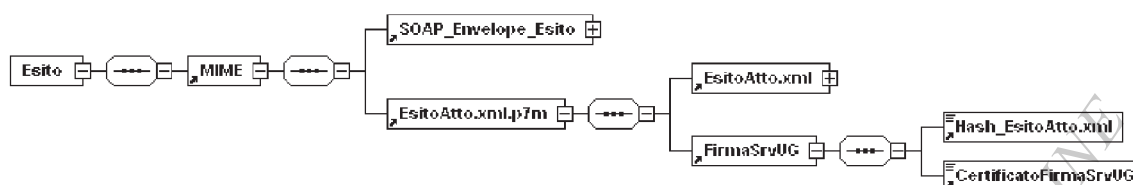



***Figura 27 – MIME di Esito***

dove la struttura SOAP_Envelope_Esito ha la seguente rappresentazione grafica:

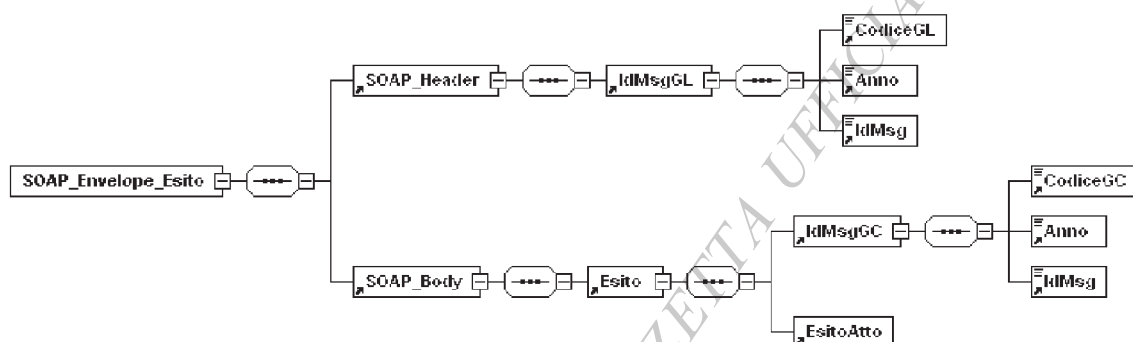



***Figura 28 – Struttura SOAP_Envelope di Esito***

Il messaggio viene ricevuto dal GC all'indirizzo identificato dalla URI http://gestorecentrale.processotelematico.giustizia.it/esitoatto.asp.

**1. SOAP:Envelope della busta di Esito**

La struttura contiene a livello di header l'identificativo univoco del messaggio di *Esito* generato dall'GL.

Il body della struttura ha un elemento, denominato Esito, contenente:

| | | |
|---|---|---|
| *IdMsgGC* | = | È l'identificativo univoco del messaggio di *Deposito atto* generato dal GC. |
| *EsitoAtto* | = | Referenzia il file EsitoAtto.xml.p7m allegato nel MIME. |

**2. File EsitoAtto.xml.p7m**

Il file *EsitoAtto.xml.p7m* generato presso l'UG e firmato dall'UG stesso (firma server), trasporta le informazioni che comunicano all'Avvocato l'esito dell'atto.

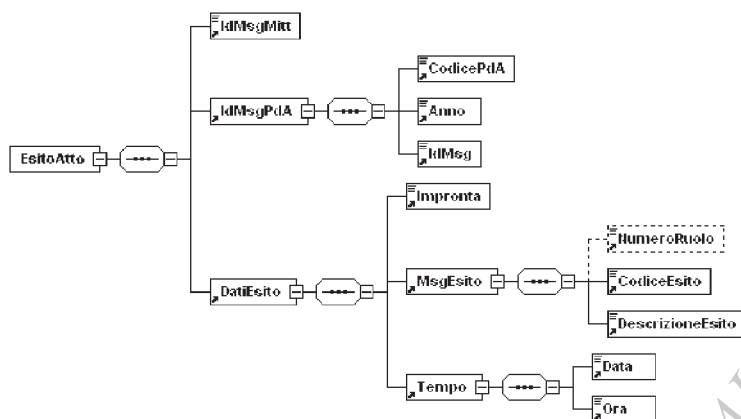



***Figura 29 - EsitoAtto.xml***

Benché il file non sia cifrato, il GC non esegue alcun controllo sulla sua struttura e sui suoi contenuti, per il cui dettaglio si rimanda al documento di "Analisi funzionale del Processo Telematico".

### *3.2.2 Il messaggio di risposta "comunicazione esito"*

Quando il GC riceve un messaggio di *esito atto*, attraverso l'identificativo del messaggio (*IdMsgGC*) ricava tutte le informazioni necessarie per recapitare il messaggio (Avvocato destinatario, PdA di appartenenza).

Il messaggio contiene allegato all'interno della struttura MIME il file EsitoAtto.xml.p7m firmato dall'UG.

***Figura 30 – MIME di Comunicazione esito***

# 4 INVIO DI UNA COMUNICAZIONE DI CANCELLERIA

La funzione di *invio comunicazione (o biglietto) di cancelleria* prevede un flusso di trasmissione di una comunicazione da un GL, fino al dominio di Posta Certificata del Processo Telematico del PdA gestore della CPECPT dell'Avvocato destinatario, e un flusso di risposta, di direzione opposta, innescato dalla produzione automatica della *ricevuta breve di avvenuta consegna*, che viene restituita al GL mittente munita dell'attestazione temporale emessa dal GC al momento della sua ricezione.

Benché al di fuori del contesto di analisi del presente documento, giova ricordare che il flusso del biglietto di cancelleria è originato dall'azione di un cancelliere e che nell'ambito dei meccanismi di scambio previsti dalla Posta Certificata si generano ulteriori due ricevute:

- la *ricevuta di accettazione*, emessa dal server di dominio del sistema di Posta Certificata del Processo Telematico del GC, depositata nella casella di Posta Certificata dell'UG mittente, presso il GC;
- la *ricevuta di presa in carico*, emessa dal server di dominio del sistema di Posta Certificata del Processo Telematico del PdA, destinata al corrispondente server mittente del GC.

I messaggi di Posta Certificata del Processo Telematico relativi alla funzione di *invio biglietto di cancelleria* vengono spediti alle CPECPT degli Avvocati agli indirizzi **<CPECPT>@processotelematico.<dominiocertPdA>** e ricevuti sulle CPECPT degli UG presso il GC agli indirizzi **<codiceUG>@processotelematico.giustiziacert.it**.

I messaggi prodotti dal GC sono conformi allo standard previsto dal sistema di Posta Certificata.

La sequenza dei messaggi scambiati con il GC nella fase di trasmissione del biglietto di cancelleria e della relativa risposta è indicata nello schema seguente:

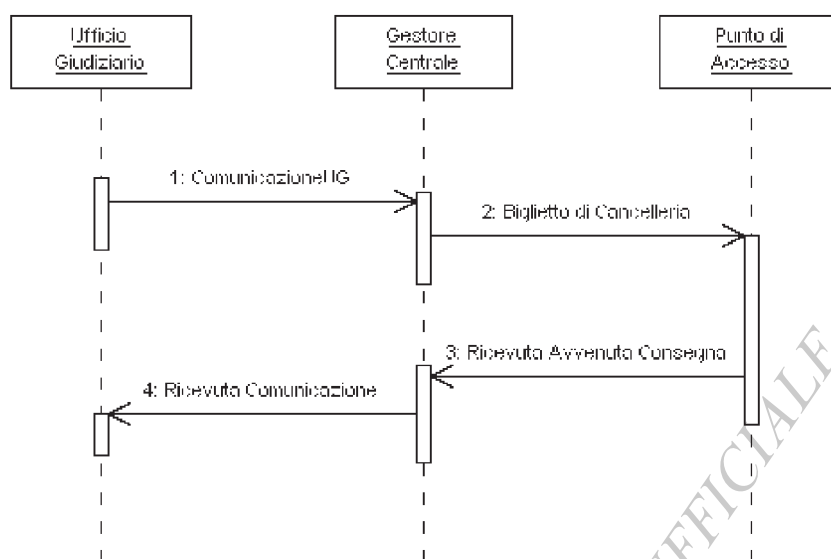



***Figura 31 – Sequence diagram dell'invio di un biglietto di cancelleria***

## *4.1 STRUTTURA DEI MESSAGGI RELATIVI ALL'INVIO DEL BIGLIETTO DI CANCELLERIA*

Nel seguito del documento viene descritta la struttura applicativa di ciascun messaggio generato dalla funzione di invio di un biglietto di cancelleria e in allegato vengono forniti i DTD di ciascuna struttura XML utilizzata.

### *4.1.1 Struttura del messaggio di "comunicazione UG"*

La struttura del messaggio di *comunicazione* proveniente da un GL è illustrata nella figura che segue:

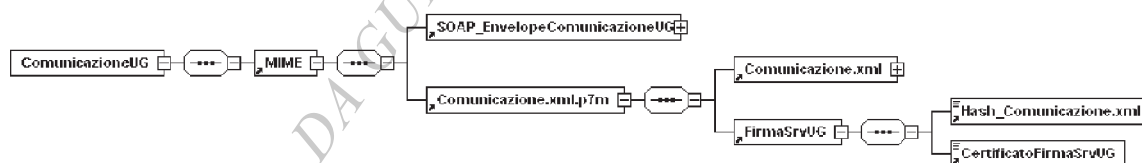



***Figura 32 – MIME di Comunicazione UG***

dove la struttura SOAP_EnvelopeComunicazioneUG ha la seguente rappresentazione grafica:

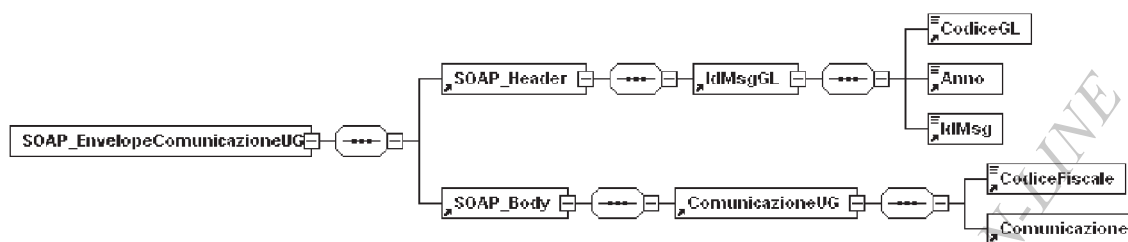



***Figura 33 – Struttura SOAP_Envelope di ComunicazioneUG***

Il messaggio viene ricevuto dal GC, all'indirizzo identificato dalla URI http://gestorecentrale.processotelematico.giustizia.it/comunicazioneUG.asp.

La transazione tra GL e GC termina con successo solo dopo che il GC ha effettuato i controlli formali sulla busta ricevuta ed ha controllato che il codice fiscale del destinatario sia presente nel ReGIndE.

La busta *ComunicazioneUG* contiene le seguenti strutture:

1. **SOAP:Envelope**

   La struttura contiene a livello di header l'identificativo univoco del messaggio generato dal GL (*IdMsgGL*).

   Il body della struttura ha un elemento, denominato ComunicazioneUG, contenente:

   *CodiceFiscale* = È l'identificativo del destinatario della comunicazione.

   *Comunicazione* = Referenzia il file Comunicazione.xml.p7m allegato nel MIME.

2. **File Comunicazione.xml.p7m**

   Il file *Comunicazione.xml.p7m* generato presso l'UG e firmato dall'UG stesso (firma server), trasporta le informazioni relative alla comunicazione da trasmettere all'Avvocato.

   Benché il file non sia cifrato, il GC non esegue alcun controllo sulla sua struttura e sui suoi contenuti, per il cui dettaglio si rimanda al documento di "Analisi funzionale del Processo Telematico".

### *4.1.2 Struttura del messaggio di "biglietto cancelleria"*

Ricevuta la comunicazione da parte del GL, il servizio SMTP del GC genera un messaggio di Posta Certificata del Processo Telematico contenente in allegato il file Comunicazione.xml.p7m.

Il messaggio riporta come destinatario, la CPECPT dell'Avvocato corrispondente al codice fiscale trasmesso, e come mittente la CPECPT dell'UG dal quale è stata ricevuta la comunicazione.

Tale messaggio, secondo i meccanismi standard di Posta Certificata, viene acquisito dal server di dominio del GC, imbustato in un messaggio di trasporto e spedito al server di dominio di Posta Certificata del PdA. A seguito di tali operazioni il server SMTP di Posta Certificata del GC restituisce nella CPECPT dell'UG mittente una *ricevuta breve di accettazione* che segnala l'effettiva spedizione del messaggio la cui struttura è rappresentata di seguito:

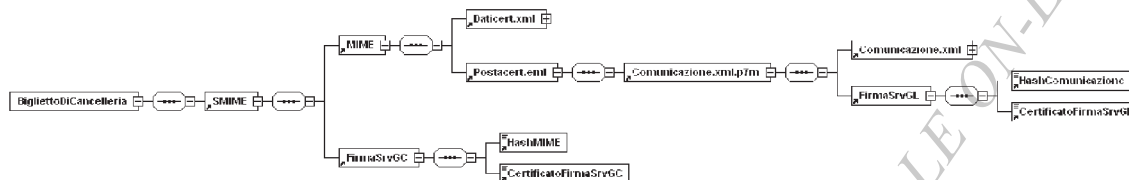



***Figura 34 – S/MIME di Biglietto di cancelleria***

### *4.1.3 Struttura del messaggio di "ricevuta comunicazione"*

All'atto della ricezione nella CPECPT dell'UG mittente della *ricevuta breve di avvenuta consegna* il GC genera automaticamente l'attestazione temporale di tale evento.

Il file Attestazione.xml.p7m insieme con la *ricevuta breve di avvenuta consegna* viene imbustato in un messaggio di *Ricevuta comunicazione* che presenta la struttura appresso schematizzata:

***Figura 35 – MIME di Ricevuta comunicazione***

dove la struttura SOAP_Envelope_RicevutaComunicazione ha la seguente rappresentazione grafica:

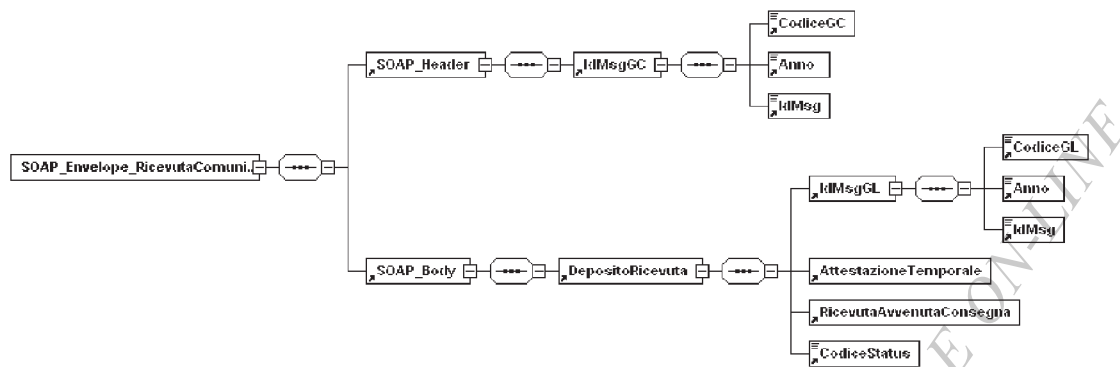



***Figura 36 – Struttura SOAP_Envelope di RicevutaComunicazione***

Il messaggio viene spedito dal GC all'indirizzo identificato dalla URI http://<codiceGL>.processotelematico.giustizia.it/<servizioRicevutaComunicazione>.

La busta *RicevutaComunicazione* contiene le seguenti strutture:

1. **SOAP:Envelope**

   La struttura contiene a livello di header il codice univoco generato dal GC per identificare il messaggio ricevuto.

   Il body della struttura ha un elemento, denominato *DepositoRicevuta* contenente:

| | | |
|---|---|---|
| *IdMsgGL* | = | E' l'identificativo della comunicazione trasmessa dall'UG. |
| *AttestazioneTemporale* | = | Referenzia il file Attestazione.xml.p7m, generato e firmato dal GC, allegato nel MIME. |
| *RicevutaAvvenutaConsegna* | = | Referenzia il file RicevutaAvvenutaConsegna.eml ricevuto dal PdA, allegato nel MIME. |
| *CodiceStatus* | = | Contiene il codice dello status professionale dell'Avvocato destinatario della comunicazione (attivo, sospeso, radiato). |

2. **File Attestazione.xml.p7m**

   Il file Attestazione.xml.p7m ha la struttura presentata in ***Figura 22*** ed è firmato dal GC (firma server). Il contenuto informativo di tale file è il seguente:

- IdMsgSMTP.

  *IdMsgSMTP* = Contiene il valore del parametro SMTP Message-ID del messaggio di *ricevuta breve di avvenuta consegna*

- IdMsgMitt e IdMsgPdA.

  In questo caso non sono valorizzati (questi elementi sono alternativi rispetto al precedente).

- DatiAttestazione.

| | |
|---|---|
| *DatiAttestazione* = | Contiene l'impronta della busta di *ricevuta breve avvenuta consegna* (nel formato S/MIME) e la data e ora dell'evento di attestazione temporale |

**3. File RicevutaAvvenutaConsegna.eml**

E' il messaggio di *ricevuta breve di avvenuta consegna* così come ricevuta dal dominio di Posta Certificata del Processo Telematico del PdA.

# 5 CONSULTAZIONE WEB (POLISWEB)

Il sistema PolisWeb fornisce un'interfaccia applicativa per l'integrazione delle funzionalità di Consultazione per il Processo Telematico, presso un Punto di Accesso (Modalità Internet).

L'interfaccia applicativa permette l'attivazione di PolisWeb, installato presso un Punto di Accesso, a seguito dell'autenticazione effettuata e delegata al Punto di Accesso stesso.

A seguito dell'autenticazione di un utente da parte del Punto di Accesso, PolisWeb può essere attivato tramite l'interfaccia applicativa che espone e attraverso la quale riceve e condivide i parametri identificativi dell'utente e della sessione utente.

## *5.1 CARATTERISTICHE DI POLISWEB*

PolisWeb per il Processo Telematico è costituita da un'applicazione Web basata sul modello J2EE.

La soluzione architetturale e tecnologica di PolisWeb prevede l'utilizzo del Web Server Apache e di Jakarta Tomcat come container per la tecnologia java utilizzata (Jsp, Servlet, Bean).

Per il progetto del Processo Telematico si è adottato Linux come sistema operativo dei sistemi server, e quindi anche per PolisWeb presso il Punto di Accesso è consigliata l'adozione di Linux.

PolisWeb integrato e configurato presso il Punto di Accesso, non necessita di un Database. Le informazioni di configurazione sono definite all'interno di file nel filesystem. Le informazioni relative agli utenti non sono gestite da PolisWeb ma ricevute, e ritenute valide, dall'interfaccia per il Punto di Accesso.

Si precisa comunque, date le caratteristiche open-source dei prodotti tecnologici utilizzati per PolisWeb, che il sistema operativo Microsoft Windows può essere valutato come ambiente server per il PolisWeb presso il Punto di Accesso.

La documentazione rilasciata dal'RTI relativa all'installazione e configurazione di PolisWeb per Processo Telematica sarà relativa al sistema operativo Linux.

Tra le caratteristiche di PolisWeb, si ricorda inoltre la sua configurabilità. La configurabilità di PolisWeb nella Fase 1 del Processo Telematico, permette al Punto di Accesso una minima personalizzazione dell'Interfaccia Grafica per l'utente. Con la personalizzazione dei loghi, delle intestazioni, dei colori è possibile, ad esempio, allineare l'interfaccia utente di PolisWeb con alcune preferenze adottate dal Punto di Accesso.

Nei paragrafi che seguono sono fornite le informazioni relative all'Interfaccia Applicativa tra Punto di Accesso e PolisWeb, con l'indicazione dei protocolli di comunicazione adottati.

Nella tabella seguente sono riepilogate le caratteristiche tecnologiche di PolisWeb.

| **CARATTERISTICA** | **DESCRIZIONE** | |
|---|---|---|
| Tipo Applicazione | Applicazione Web Java | |
| Sistema Operativo | Linux (Windows 2000 Server) | SERVER |
| Java Virtual Machine | 1.4.2 | SERVER |
| Web Server | Apache. | SERVER |
| Web Container | Tomcat. | SERVER |
| Database | Non necessario. | SERVER |
| Configurabilità | Alcune caratteristiche del Front-End. | SERVER |
| Interfaccia Applicativa | Parametri Intestazione Richieste http<br>Parametri Intestazione Risposte http | |
| Protocollo PA-PW | http | |
| Protocollo PW-GC | https con mutua autenticazione | |
| Browser supportati | Microsft Explorer, Netscape, Mozilla. | CLIENT |
| Configurazione browser | Utilizzati Coockie e java script lato client. | CLIENT |

***Tabella 1 - Caratteristiche di PolisWeb per il Punto di Accesso***

## *5.2 ARCHITETTURA E FLUSSI DI COLLOQUIO TRA PUNTO ACCESSO E POLISWEB*

PolisWeb presso il Punto di Accesso permette agli utenti del Processo Telematico di accedere alle informazioni di Back-End presso gli Uffici Giudiziari attraverso il Punto di Accesso e il Gestore Centrale (Modalità Internet).

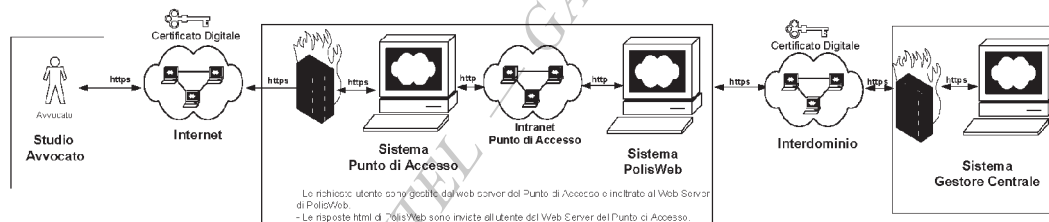



***Figura 37 – Architettura per PolisWeb nel Punto di Accesso***

Si precisa che il precedente schema è stato volutamente rappresentato con un'immagine e non attraverso un diagramma UML, per dare la percezione schematica della relazione tra il sistema del Punto di Accesso e PolisWeb. Si precisa che essendo Polis Web multipiattaforma, l'applicazione potrà essere opzionalmente installata sulla stessa macchina del Punto di Accesso. Nei paragrafi successivi è riportata la descrizione dei flussi tra PA e PW attraverso un diagramma di sequenza.

Il Punto di Accesso si interpone tra le richieste dell'utente e PolisWeb. Le richieste effettuate dall'utente, tramite browser web, sono autenticate dal Punto di Accesso (smart-card). A seguito dell'autenticazione dell'utente, il Punto di Accesso può attivare PolisWeb tramite l'interfaccia applicativa esposta.

PolisWeb è installato presso la "Server Farm" del punto di accesso e isolato verso l'esterno (Internet, Interdominio, altro).

Nell'analisi dei requisiti di colloquio tra il Punto di Accesso e PolisWeb si evidenziano le seguenti esigenze:

- Attivazione di una sessione utente di PolisWeb.
- Richiesta di Consultazione Informazioni di PolisWeb.
- Chiusura di una sessione utente di PolisWeb.
- Gestione delle eccezioni.

I diagrammi di sequenza, di seguito illustrati, permettono di definire il flusso di colloquio tra il Punto di Accesso e PolisWeb.

**<u>Attivazione Sessione Utente di PolisWeb</u>**

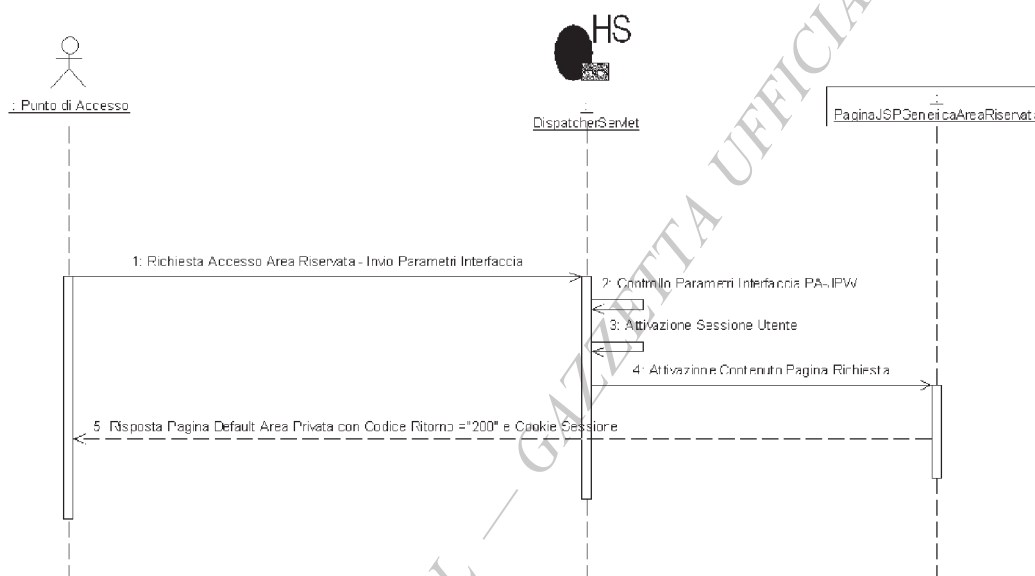



***Figura 38 – Sequenza Messaggi PA / FE-PW-PA- Attivazione Sessione***

*<u>Spiegazione:</u>*

- A seguito della richiesta di accesso all'area Privata di PolisWeb da parte di un utente autenticato dal Punto di Accesso, il Punto di Accesso si interfaccia a PolisWeb chiedendo l'attivazione di una sessione utente. L'interfaccia applicativa di PolisWeb per l'attivazione della sessione utente prevede una serie di parametri descritti in dettaglio nel seguito di questa sezione del documento.
- PolisWeb, a seguito della richiesta di attivazione di una sessione utente effettua il controllo dei parametri dell'interfaccia di attivazione, forniti dal Punto di Accesso. L'interfaccia di attivazione e i parametri di interscambio con PolisWeb sono descritti nel paragrafo 7.2.13. (JPW_COD_FISCALE, JPW_COGNOME, JPW_NOME, JPW_DT_ULTIMO_ACCESSO, JPW_INFO_PA).
- Superati i controlli dei parametri (in caso contrario è attivata un'eccezione applicativa da parte di PolisWeb trattata in particolare nell'ultimo diagramma), PolisWeb attiva la sessione utente in base all'utente identificato dal Codice Fiscale ricevuto come parametro.

L'attivazione della sessione prevede il controllo da parte di PolisWeb che, per il Codice Fiscale corrente, non risulti già attiva una sessione (eccezione).

- A seguito dell'attivazione della sessione utente, PolisWeb individua la pagina di default da presentare all'utente a seguito dell'attivazione nell'area privata.
- PolisWeb infine risponde al Punto di Accesso con la pagina html, indicando il Codice Ritorno 200 per la corretta attivazione della sessione utente e il cookie per le informazioni identificative della sessione di PolisWeb.

**Consultazione Informazioni di PolisWeb**

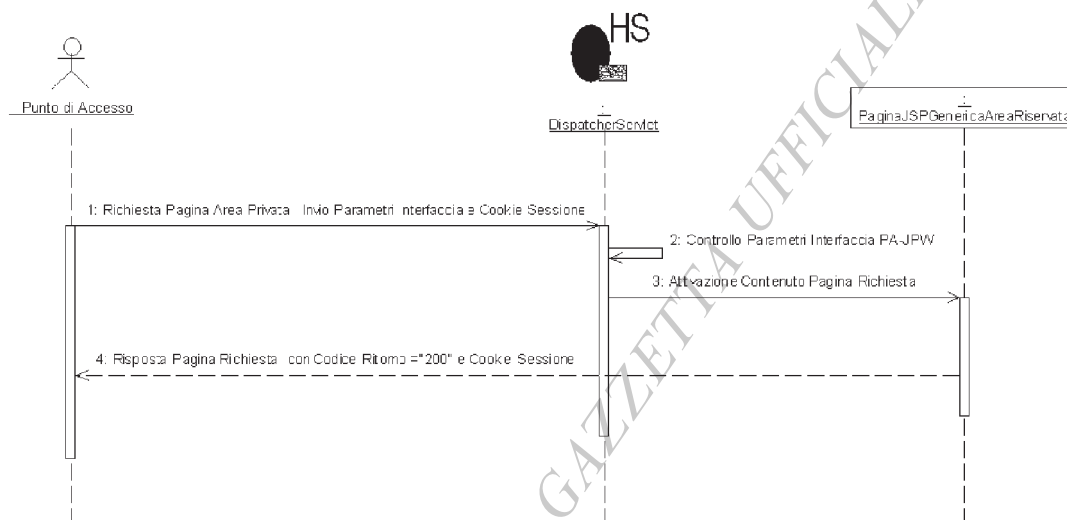



***Figura 39 – Sequenza Messaggi PA / FE-PW-PA- Consultazione***

*Spiegazione:*

- Il dialogo tra Punto di Accesso e PolisWeb è basato sullo scambio delle informazioni previste dall'interfaccia applicativa di PolisWeb per ogni richiesta effettuata dal Punto di Accesso. Il Punto di Accesso richiede una singola pagina di Consultazione di PolisWeb, fornendo i parametri dell'interfaccia e il Cookie di sessione ricevuto da PolisWeb dopo l'attivazione della sessione utente attiva.
- PolisWeb controlla i parametri di interfaccia, che prevedono anche il cookie di sessione utente. Il cookie deve determinare in PolisWeb una corrispondenza tra una sessione valida e associata in precedenza al Codice Fiscale, ricevuto nella richiesta corrente (altrimenti Eccezione).
- PolisWeb determina il contenuto html da fornire al Punto di Accesso, in base alla funzione richiesta.
- PolisWeb infine risponde al Punto di Accesso con la pagina html, indicando il Codice Ritorno 200 per la corretta attivazione della sessione utente e il cookie per le informazioni identificative della sessione di PolisWeb.

**Chiusura Sessione Utente di PolisWeb**

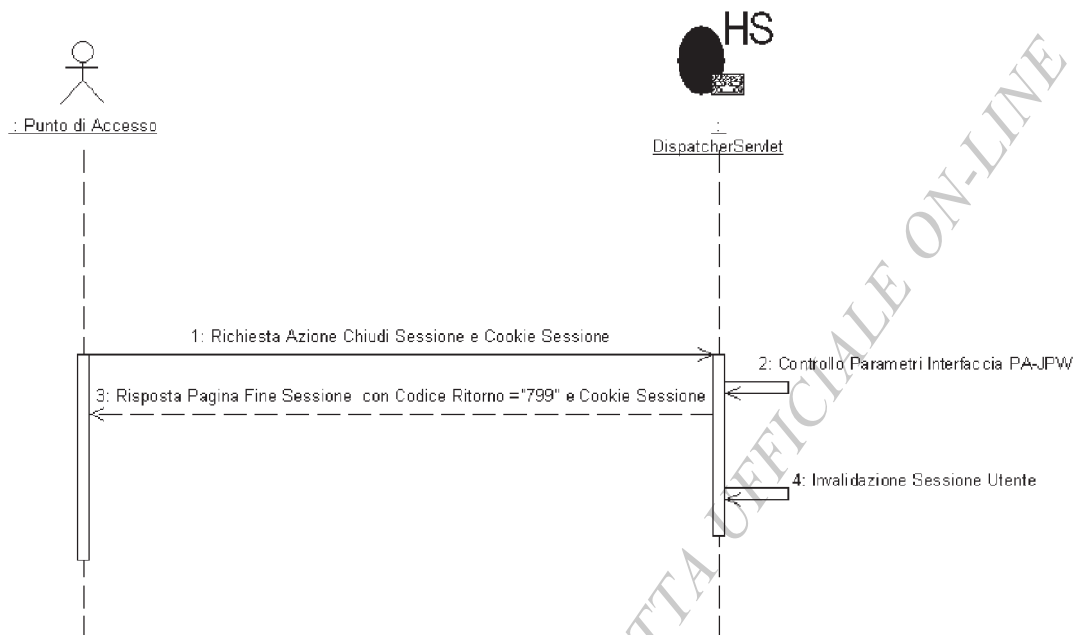



***Figura 40 – Sequenza Messaggi PA / FE-PW-PA- Chiusura Sessione***

*Spiegazione:*

- La chiusura della sessione utente in PolisWeb può avvenire attraverso la richiesta diretta della funzione di logout da parte dell'utente, attraverso l'interfaccia utente di PolisWeb fornita all'utente dal Punto di Accesso. PolisWeb espone al Punto di Accesso, un'interfaccia applicativa per richiedere direttamente a PolisWeb la chiusura della sessione utente. Questa funzionalità può risultare utile nel caso in cui il Punto di Accesso determini una propria chiusura di sessione con l'utente (timeout).
- PolisWeb a seguito della richiesta di chiusura di una sessione utente, da Parte del Punto di Accesso, controlla la corrispondenza tra cookie di sessione attivata e il codice fiscale corrispondente (Eccezione se non corrisponde).
- PolisWeb, a seguito della chiusura di una propria sessione utente (anche nel caso di richiesta da parte dell'utente), risponde al Punto di Accesso con un contenuto html, riportando il Codice Ritorno 799 ad indicare l'avvenuta chiusura della sessione utente.

**Eccezione PolisWeb in caso di ricezione di parametri errati dal Punto di Accesso**

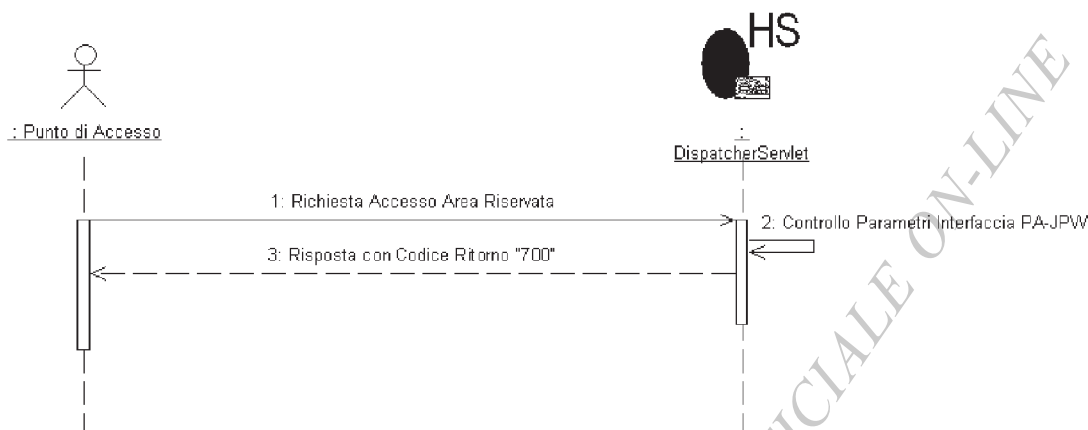



*Figura 41 – Sequenza Messaggi PA / FE-PW-PA- Eccezione Parametri Errati*

Come descritto nei diagramma di sequenza precedenti, in caso di controlli non validi PolisWeb determina una Eccezione segnalata al Punto di Accesso attraverso il Codice di Ritorno. L'elenco dei codici previsti è riportato successivamente, e nel caso dei parametri errati è impostato a 700.

**Eccezione PolisWeb in caso di richiesta di attivazione di una sessione per utente connesso**

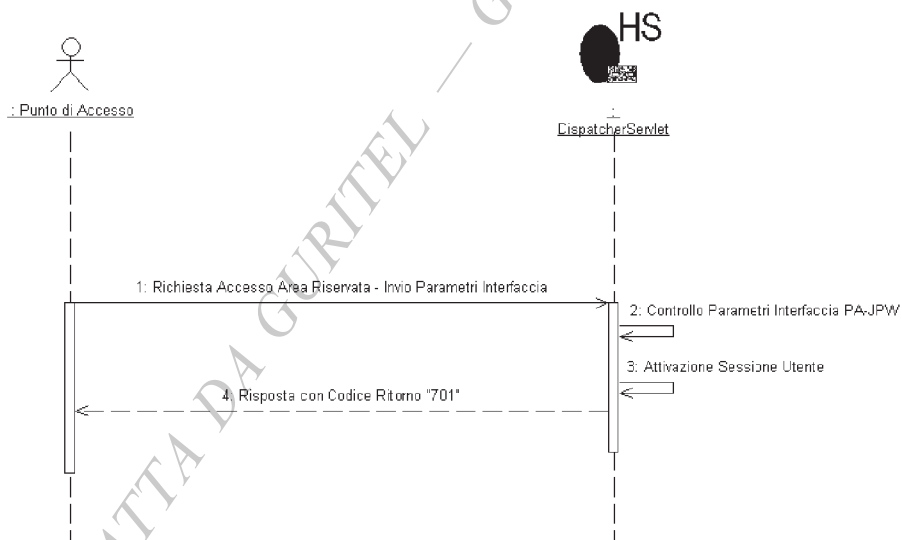



*Figura 42 – Sequenza Messaggi PA / FE-PW-PA- Eccezione Utente Connesso*

Nel caso di richiesta dell'attivazione per un utente che risulta già connesso il codice di ritorno impostato da PolisWeb per il Punto di Accesso è uguale a 701.

## *5.3 INTERFACCE PER IL PUNTO DI ACCESSO*

Sono descritte le informazioni di interscambio tra il Punto di Accesso e PolisWeb, relative a:

- Richiesta attivazione di una sessione utente di PolisWeb da parte del Punto di Accesso.
- Risposta di PolisWeb al Punto di Accesso , alla richiesta di attivazione di una sessione utente.
- Richiesta a PolisWeb delle pagine del front-end di consultazione dell'area privata, da parte del Punto di Accesso.
- Risposta di PolisWeb alla richiesta da parte del Punto di Accesso delle pagine del front-end di consultazione dell'area privata.
- Richiesta di chiusura di una sessione utente di PolisWeb da parte del Punto di Accesso.
- Risposta di PolisWeb al Punto di Accesso, alla richiesta di chiusura di una sessione utente.
- Risposte di PolisWeb al Punto di Accesso, in caso di Eccezione.

### *5.3.1 Richiesta "Attivazione Sessione Utente PolisWeb"*

Per l'attivazione di una sessione utente di PolisWeb, da parte del Punto di Accesso è fornita un'interfaccia applicativa che prevede l'utilizzo del protocollo http tra PA e PW.

Il PA (Client) invia la richiesta di login verso il server PolisWeb aggiungendo nella testata della richiesta client le informazioni dell'utente, individuate a seguito di un'autenticazione valida con smart-card.

Sono di seguito fornite le modalità di attivazione dell'interfaccia applicativa di PolisWeb e un esempio del relativo messaggio di richiesta http inviata dal PA a PW.

Richiesta http inviata dal Punto di Accesso a PolisWeb per l'attivazione della sessione utente: http://hostpwpa/pwprivate?action=Login

**Esempio di Messaggio di Richiesta http inviata dal Punto di Accesso a PolisWeb – Attivazione Sessione**

```
POST /pwprivate?action=Login HTTP/1.0 <CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, */*<CR><LF>
Accept-Language: it<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) <CR><LF>
Host: jpolisweb:8081<CR><LF>
JPW_COD_FISCALE: CPRGRGXXXXXXXXXX<CR><LF>
JPW_COGNOME: YYYYYYYY<CR><LF>
JPW_NOME: ZZZZZZZZZ<CR><LF>
JPW_DT_ULTIMO_ACCESSO: GG/MM/YYYY HH24:MI:SS<CR><LF>
JPW_INFO_PA: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>
```

*Spiegazione:*

Il Punto di Accesso fornisce nell'intestazione del messaggio di richiesta http (Header Http_Request) inviato a PolisWeb i seguenti parametri:

- JPW_COD_FISCALE: rappresenta il Codice Fiscale dell'utente autentificato dal Punto di Accesso. Questo parametro è obbligatorio. Il Codice Fiscale dell'utente è utilizzato da

PolisWeb per l'attivazione della sessione utente. Per ogni richiesta di informazione è verificata la presenza di una sessione attiva valida in PolisWeb.

- JPW_COGNOME: rappresenta il Cognome dell'utente. Permette di visualizzare sull'Interfaccia Utente di PolisWeb il nominativo dell'utente attivo nella sessione visualizzata nel browser .
- JPW_NOME: rappresenta il Nome dell'utente. Vedi JPW_COGNOME.
- JPW_DT_ULTIMO_ACCESSO: rappresenta la data di ultimo accesso da parte dell'utente al sistema di consultazione PolisWeb per il Processo Telematica dal Punto di Accesso. Permette di visualizzare sull'Interfaccia Utente di PolisWeb la data di ultimo accesso dell'utente e di poter utilizzare correttamente la consultazione dell'Agenda relativa agli ultimi eventi.
- JPW_INFO_PA: rappresenta un parametro, utile al Punto di Accesso, per l'interscambio di informazioni con PolisWeb. Questo parametro non è necessario a PolisWeb, ma è reso disponibile al Punto di Accesso. Questa informazione è restituita, al Punto di Accesso, nel messaggio di risposta. Un utilizzo pratico può essere ad esempio ricevere e restituire una chiave della sessione utente del Punto di Accesso.

### *5.3.2 Risposta PolisWeb alla richiesta di "Attivazione Sessione Utente PolisWeb"*

PolisWeb alla richiesta di attivazione di una nuova sessione utente risponde al client del Punto di Accesso con un messaggio riportante nella header http i parametri di interfaccia applicativa e il cookie relativo alla sessione utente attivata in PolisWeb.

**Esempio di Risposta http resituita da PolisWeb al Punto di Accesso**

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=iso-8859-1
Connection: close
Date: Tue, 21 Oct 2003 16:03:01 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Set-Cookie: JSESSIONID= A889EA5555C7A387F36A7A2892045FFD;Path=/
JPW_CODICE_RITORNO: 200<CR><LF>
JPW_DESCR_SEGNALAZIONE: OK<CR><LF>
JPW_INFO_PA: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>
```

*Spiegazione:*

- Set-Cookie: JSESSIONID= A889EA5555C7A387F36A7A2892045FFD;Path=/: rappresenta l'informazione identificativa della sessione utente di PolisWeb. Questa informazione deve essere ritornata a PolisWeb nelle successive richieste, per associare correttamente utente e sessione utente.
- JPW_CODICE_RITORNO: rappresenta il codice di ritorno previsto da PolisWeb, in base alla codifica riportata nella tabella …vedi oltre. Nel caso di corretta attivazione della nuova sessione utente assume il valore "200". Per quanto riguarda le situazioni in cui PolisWeb non riesce ad attivare, o determinare, la sessione utente (ad. Es. già collegato) consultare il trattamento delle risposte "*Eccezioni*", analizzate in ultimo.
- JPW_DESCR_SEGNALAZIONE: rappresenta una stringa di descrizione del codice di ritorno. Nel caso di corretta attivazione della sessione utente assume il valore di "OK".

- JPW_INFO_PA: è il parametro ricevuto nella richiesta del Punto di Accesso. Questo parametro è restituito, senza nessun trattamento, in risposta.

Si precisa che la risposta http di PolisWeb contiene oltre ai parametri di interscambio previsti con il PA, anche l'html della prima pagina consultabile dall'utente a seguito dell'attivazione della sessione (pagina di default).

Di seguito vengono elencati i Codici di Ritorno individuati ad oggi:

| JPW_COD_RITORNO | JPW_DESCR_SEGNALAZIONE | COMMENTI | PDA |
|---|---|---|---|
| 200 | OK | | Si |
| 700 | Parametro invalido o non presente. | Un parametro fondamentale per l'elaborazione non e' presente o è invalido. Esempio mancanza del codice fiscale o dello username nella richiesta. | Si |
| 701 | Utente già connesso. | E' stata trovata un'altra sessione attiva per lo stesso Codice Fiscale. | Si |
| 709 | Sessione errata. | Le informazioni di sessione non corrispondono ad una sessione valida. | Si |
| 710 | Informazioni sessione errata. | Le informazioni di sessione non corrispondono con il Codice Fiscale associato. | Si |
| 799 | Chiusura sessione. | L'utente ha richiesto una chiusura della sessione. | Si |

***Tabella 2 - Codici Ritorno FE-PW-PA***

### *5.3.3 Richiesta "Pagine Area Privata Consultazione PolisWeb"*

Il Punto di Accesso successivamente all'attivazione della sessione di PolisWeb, deve inoltrare tutte le richieste dell'utente a PolisWeb dopo aver aggiunto all'intestazione della richiesta http (header http request) i parametri definiti dall'interfaccia di attivazione di PolisWeb.

**Esempio Messaggio di Richiesta http inviata dal Punto di Accesso a PolisWeb – Consultazione Informazioni**

POST /forms/RicercaFascicoliPersonali;**jsessionid=A889EA5555C7A387F36A7A2892045FFD**?action=ElencoFascicoliPersonali HTTP/1.0<CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*<CR><LF>
Referer: http://localhost:8081/pwprivate?action=Login<CR><LF>
Accept-Language: it<CR><LF>
Content-Type: application/x-www-form-urlencoded<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) <CR><LF>
Host: localhost:8081<CR><LF>
Content-Length: 33<CR><LF>
Pragma: no-cache<CR><LF>
**Cookie: JSESSIONID**=A889EA5555C7A387F36A7A2892045FFD<CR><LF>
**JPW_COD_FISCALE**: CPRGRGXXXXXXXXX<CR><LF>
**JPW_COGNOME**: YYYYYYYY<CR><LF>
**JPW_NOME**: ZZZZZZZZZ<CR><LF>
**JPW_DT_ULTIMO_ACCESSO**: GG/MM/YYYY HH24:MI:SS<CR><LF>

<CR><LF>

*Spiegazione:*

- Cookie: JSESSIONID=A889EA5555C7A387F36A7A2892045FFD: rappresenta l'informazione identificativa della sessione utente in PolisWeb, ricevuta in risposta dal PA dopo la richiesta di attivazione della sessione utente.

- JPW_COD_FISCALE: rappresenta il Codice Fiscale dell'utente. E' obbligatorio. PolisWeb controlla l'associazione del Codice Fiscale con la sessione utente identificata con le informazioni del cookie.
- JPW_COGNOME, JPW_NOME, JPW_DT_ULTIMO_ACCESSO: vedi descrizione fornita nella richiesta di attivazione della sessione.

### *5.3.4 Risposta di PolisWeb alla richiesta "Pagine Area Privata Consultazione PolisWeb".*

La risposta fornita da PolisWeb è nello stesso formato della risposta descritta per la richiesta di attivazione della sessione utente. La risposta differisce nel contenuto l'html della pagina di consultazione richiesta.

### *5.3.5 Richiesta "Chiusura Sessione Utente PolisWeb"*

Sono di seguito forniti le modalità di attivazione dell'interfaccia applicativa di PolisWeb per la chiusura di una sessione utente, e un esempio del relativo messaggio di richiesta http inviata dal PA a PW.

Richiesta http inviata dal Punto di Accesso a PolisWeb per la chiusura della sessione utente: <u>http://hostpwpa/pwprivate?action=Logout</u>

**<u>Esempio di Messaggio di Richiesta http inviata dal Punto di Accesso a PolisWeb – Chiusura Sessione</u>**

POST /pwprivate;**jsessionid=A889EA5555C7A387F36A7A2892045FFD**?action=Logout HTTP/1.0 <CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*<CR><LF>
Referer: http://localhost:8081/pwprivate?action=Login<CR><LF>
Accept-Language: it<CR><LF>
Content-Type: application/x-www-form-urlencoded<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) <CR><LF>
Host: localhost:8081<CR><LF>
Content-Length: 33<CR><LF>
Pragma: no-cache<CR><LF>
**Cookie: JSESSIONID=**A889EA5555C7A387F36A7A2892045FFD<CR><LF>
**JPW_COD_FISCALE**: CPRGRGXXXXXXXXX<CR><LF>
**JPW_COGNOME**: YYYYYYYY<CR><LF>
**JPW_NOME**: ZZZZZZZZZ<CR><LF>
**JPW_DT_ULTIMO_ACCESSO**: GG/MM/YYYY HH24:MI:SS<CR><LF>
<CR><LF>

Analogamente ai messaggi di richiesta precedenti, per richiedere la chiusura forzata di una specifica sessione utente, occorre attivare l'azione di Logout indicando le informazioni relative all'utente (Cookie e Codice Fiscale).

### *5.3.6 Risposta PolisWeb per richiesta "Chiusura Sessione Utente PolisWeb"*

PolisWeb alla richiesta di chiusura di una sessione utente, dopo aver chiuso la sessione utente, risponde al client del Punto di Accesso con un messaggio riportante nella header http i parametri di interfaccia applicativa previsti

.

**Esempio di Risposta http restituita da PolisWeb al Punto di Accesso per Richiesta Chiusura Sessione**

HTTP/1.1 200 OK
Content-Type: text/html; charset=iso-8859-1
Connection: close
Date: Tue, 21 Oct 2003 16:03:01 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Set-Cookie: **JSESSIONID= A889EA5555C7A387F36A7A2892045FFD**;Path=/
**JPW_CODICE_RITORNO**: 799<CR><LF>
**JPW_DESCR_SEGNALAZIONE**: OK<CR><LF>
**JPW_INFO_PA**: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>

*Spiegazione:*

JPW_COD_RITORNO: con il valore di Codice di Ritorno "799" il punto di accesso ha la conferma della chiusura della sessione e può redirigere l'utente in una funzionalità del Punto di Accesso.

### *5.3.7 Eccezioni*

Con il concetto di eccezione, relativamente all'interfaccia tra PA e PW, si intendono situazioni in cui ad una precisa richiesta del Punto di Accesso PolisWeb non può rispondere come dovuto. Queste eccezioni possono essere dovute sia ad errate impostazione dei parametri di attivazione del Punto di Accesso che per condizioni di stato di PolisWeb. Le eccezioni ad oggi individuate sono le seguenti:

- 700 – Parametro invalido o non presente. Un parametro dell'interfaccia di attivazione di PolisWeb, fondamentale per l'elaborazione della richiesta, non è fornito o è invalido.
- 701 – Utente già connesso. Nell'elaborazione della richiesta di attivazione di una nuova sessione utente, è trovata un'altra sessione attiva per lo stesso Codice Fiscale.
- 709 – Sessione errata. Le informazioni di sessione fornite a PolisWeb attraverso l'interfaccia di attivazione, non corrispondono ad una sessione valida.
- 710 – Informazione sessione errata. Le informazioni di sessione fornite a PolisWeb attraverso l'interfaccia di attivazione, non corrispondono con il Codice Fiscale associato.

**Esempio di Risposta http restituita da PolisWeb al Punto di Accesso in caso di Eccezione**

HTTP/1.1 200 OK
Content-Type: text/html; charset=iso-8859-1
Connection: close
Date: Tue, 21 Oct 2003 16:03:01 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Set-Cookie: **JSESSIONID= A889EA5555C7A387F36A7A2892045FFD**;Path=/
**JPW_CODICE_RITORNO**: 700<CR><LF>
**JPW_DESCR_SEGNALAZIONE**: Parametro invalido o non presente.<CR><LF>
**JPW_INFO_PA**: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>

*Spiegazione:*

JPW_COD_RITORNO: con il valore di Codice di Ritorno "700" il punto di accesso ha l'evidenza di una situazione di "Eccezione". In caso di un'eccezione il Punto di Accesso può intercettare e condizionare il flusso http. La risposta di PolisWeb contiene comunque l'html di visualizzazione dell'eccezione riscontrata.

### *5.3.8 Sicurezza Punto Di Accesso, PolisWeb e Gestore Centrale*

Per quanto concerne gli aspetti di sicurezza tra il **Punto di Accesso e PolisWeb** si precisa quanto segue:

- Il sistema PolisWeb è installato e configurato all'interno della Intranet del Punto di Accesso.
- Il sistema PolisWeb non deve essere accessibile dall'esterno della Intranet del Punto di Accesso (Internet, Interdominio, altro).
- Il Punto di Accesso e PolisWeb utilizzano il protocollo di comunicazione http per lo scambio dei messaggi.
- PolisWeb delega l'autenticazione degli utenti al Punto di Accesso (Smart-Card).

Per quanto concerne gli aspetti di sicurezza tra il **PolisWeb e il Gestore Centrale**, si precisa che utilizzano il protocollo Https su SSL con autenticazione client per lo scambio delle informazioni. In particolare l'applicazione web PolisWeb, basata su tecnologia Java, sfrutta il plug-in "*JSSE – Java Security Socket Extention*" recentemente integrato nella distribuzione Java 2 SDK (a partire dalla 1.4.0).

Java Secure Socket Extension (JSSE) è un insieme di package Java che consentono comunicazioni Internet sicure. JSSE implementa una versione dei protocolli SSL e TLD e include funzionalità di cifratura dei dati, autenticazione server, integirtà dei messaggi e autenticazione client opzionale. Utilizzando JSSE, gli sviluppatori possono utilizzare, per il passaggio sicuro di dati tra client e server, qualsiasi protocollo applicativo su TCP/IP (come HTTP, Telnet, NNTP e FTP). Per ulteriori approfondimenti è possibile consultare la documentazione ufficiale disponibile sul sito http://java.sun.com/products/jsse.

### *5.3.9 Attivazione del Gestore Centrale*

Per completare questa sezione relativa a PolisWeb presso un Punto di Accesso, si riporta la modalità di attivazione delle richiste al Gestore Centrale.

Richiesta http inviata da PolisWeb al Gestore Centrale per l'individuazione delle informazioni di back-end presso un Ufficio Giudiziario, fornite dal Gestore Locale:

***https://hostgc/NomeLogicoUfficioGiudiziario/PathSoap***

Si riporta una sintetica descrizione degli elementi che compongono la richiesta di attivazione di un servizio di back-end:

**hostgc**: indirizzo telematico del Gestore Centrale configurato in PolisWeb (jpolisweb.xml).

**NomeLogicoUfficioGiudiziario**: identificativo logico dell'Ufficio Giudiziario configurato in PolisWeb (UfficiGiudiziali.xml), in base all'Ufficio indicato dall'utente nell'impostazione dei parametri di ricerca.

**PathSoap:** url relativa del servizio di backend configurato in PolisWeb e definito univocamente per l'utilizzato del Gestore Locale (jpolisweb.xml).

ALLEGATO *B*
Posta certificata del processo telematico

# *REGOLE TECNICO-OPERATIVE*
# *PER L'USO DI STRUMENTI INFORMATICI E TELEMATICI*
# *NEL PROCESSO CIVILE*

INDICE DEI CONTENUTI

## Definizioni

**Punto di accesso**

È il punto che fornisce i servizi di accesso per l'invio di messaggi di posta certificata. Il punto di accesso fornisce i servizi di accesso dell'utente, emissione della *ricevuta di accettazione*, imbustamento del *messaggio originale* nel *messaggio di trasporto*.

**Punto di ricezione**

È l'entità che riceve il messaggio all'interno di un *dominio di posta certificata*. Corrisponde alla macchina destinata alla ricezione dei messaggi per il dominio. Effettua i controlli sulla provenienza/correttezza del messaggio ed emette la *ricevuta di presa in carico*, imbusta i messaggi errati in un *messaggio di anomalia di trasporto*.

**Punto di consegna**

Effettua la consegna del messaggio nella casella di posta elettronica dell'*utente di posta certificata* destinatario. Verifica la provenienza/correttezza del messaggio, emette la *ricevuta di avvenuta consegna*.

**Ricevuta di accettazione**

È la ricevuta, contenente i *dati di certificazione*, rilasciata al mittente dal *punto di accesso* a fronte dell'invio di un messaggio di posta certificata. La ricevuta di accettazione è firmata con la chiave del *gestore di posta certificata* del mittente.

**Ricevuta di presa in carico**

È emessa dal *punto di ricezione* verso il *gestore di posta certificata* mittente per attestare l'avvenuta presa in carico del messaggio da parte del *dominio di posta certificata* di destinazione. Nella ricevuta di presa in carico sono inseriti i *dati di certificazione* per consentirne l'associazione con il messaggio a cui si riferisce.

**Ricevuta di avvenuta consegna**

Il *punto di consegna* emette al mittente la ricevuta di avvenuta consegna nel momento in cui il messaggio è inserito nella *casella di posta certificata* del destinatario. È rilasciata una ricevuta di avvenuta consegna per ogni destinatario al quale il messaggio è consegnato. La ricevuta di avvenuta consegna porta in allegato i *dati di certificazione* e, per i destinatari primari del messaggio, il *messaggio originale*.

**Ricevuta di errore di consegna**

Nel caso in cui il *punto di consegna* sia impossibilitato a consegnare il messaggio nella *casella di posta certificata* del destinatario, il sistema emette una ricevuta di errore di consegna per indicare l'anomalia al mittente del *messaggio originale*.

**Messaggio originale**

È il messaggio originale inviato da un *utente di posta certificata* prima del suo arrivo al *punto di accesso*. Il messaggio originale è consegnato all'*utente di posta certificata* di destinazione per mezzo di un *messaggio di trasporto* che lo contiene.

**Messaggio di trasporto**

È il messaggio creato dal *punto di accesso*, all'interno del quale è inserito il *messaggio originale* inviato dall'*utente di posta certificata* ed i relativi *dati di certificazione*. Il

messaggio di trasporto è firmato con la chiave del *gestore di posta certificata* mittente. Il messaggio di trasporto è consegnato immodificato nella *casella di posta certificata* di destinazione per permettere la verifica dei *dati di certificazione* da parte del ricevente.

**Messaggio di anomalia di trasporto**

Quando un messaggio errato/non di posta certificata deve essere consegnato ad un *utente di posta certificata*, il messaggio è inserito in un messaggio di anomalia di trasporto per evidenziare l'anomalia al destinatario. Il messaggio di anomalia di trasporto è firmato con la chiave del *gestore di posta certificata* del destinatario.

**Dati di certificazione**

Sono un insieme di dati che descrivono il *messaggio originale* e sono certificati dal *gestore di posta certificata* del mittente. I dati di certificazione sono inseriti nelle varie ricevute e sono trasferiti all'*utente di posta certificata* di destinazione insieme al *messaggio originale* per mezzo di un *messaggio di trasporto*. Tra i dati di certificazione sono: data ed ora di invio, mittente, destinatario, oggetto, identificativo messaggio, ecc.

**Gestore di posta certificata**

È un entità che gestisce uno o più *domini di posta certificata* con i relativi *punti di accesso, ricezione e consegna*. È titolare della chiave usata per la firma delle ricevute e dei messaggi di trasporto. Si interfaccia con altri gestori di posta certificata per l'interoperabilità con altri *utenti di posta certificata*.

**Dominio di posta certificata**

Corrisponde ad un dominio DNS dedicato alle caselle di posta elettronica degli *utenti di posta certificata*. All'interno di un dominio di posta certificata tutte le caselle di posta elettronica devono appartenere ad *utenti di posta certificata*. L'elaborazione dei messaggi di posta certificata (ricevute utente, messaggi di trasporto, ecc.) deve avvenire anche nel caso mittente e destinatario appartengano allo stesso dominio di posta certificata.

**Indice dei gestori di posta certificata**

Consiste in un server LDAP posizionato in un'area raggiungibile dai vari *gestori di posta certificata*. Contiene l'elenco dei *domini e dei gestori di posta certificata* con i relativi certificati relativi alle chiavi usate per la firma delle ricevute e dei *messaggi di trasporto*.

**Casella di posta certificata**

È una casella di posta elettronica alla quale è associata una funzione che rilascia delle *ricevute di avvenuta consegna* al ricevimento di messaggi di posta certificata. Una casella di posta certificata può essere definita esclusivamente all'interno di un *dominio di posta certificata*.

**Utente di posta certificata**

È un utente a cui è assegnata una *casella di posta certificata*. Utilizza il *punto di accesso* del proprio *gestore di posta certificata* per inviare messaggi di posta certificata.

# Elaborazione dei messaggi

## Formato dei messaggi generati dal sistema

Il sistema genera i messaggi (ricevute, messaggi di trasporto e di anomalia di trasporto) in formato MIME. I messaggi sono composti da una parte di testo descrittivo, per l'utente, e da una serie di allegati (messaggio originale, dati di certificazione, ecc.) variabili a seconda della tipologia del messaggio.
Il messaggio (composto dall'insieme delle parti descritte nelle specifiche sezioni del presente allegato) è quindi inserito in una struttura S/MIME v3 in formato CMS, firmata con la chiave privata del gestore di posta certificata. Il certificato associato alla chiave usata per la firma deve essere incluso in tale struttura. Il formato S/MIME usato per la firma dei messaggi generati dal sistema è il "multipart/signed" (formato .p7s) così come descritto nella RFC 2633 §3.4.3.
Per garantire la verificabilità della firma da parte del client di posta ricevente, il mittente del messaggio deve coincidere con quello specificato all'interno del certificato usato per la firma S/MIME. Questo meccanismo comporta che i messaggi di trasporto riportino nel campo "From" un indirizzo di posta mittente differente da quello del messaggio originale. Al fine di consentire una migliore fruibilità del messaggio da parte dell'utente finale, l'indirizzo di posta mittente del messaggio originale è inserito come "display name" mittente nel messaggio. Ad esempio, per un messaggio originale con il seguente campo "From":

```
From: "Mario Bianchi" <mario.bianchi@dominio.it>
```

**il relativo messaggio di trasporto generato avrà un campo "From" del tipo:**

```
From: "mario.bianchi@dominio.it" <posta-certificata@gestore.it>
```

Per consentire che le risposte al messaggio siano correttamente indirizzate verso il mittente originale, è necessario che l'indirizzo di quest'ultimo sia riportato nel campo "Reply-To". Qualora tale campo non fosse esplicitamente specificato nel messaggio originale, il sistema che genera il messaggio di trasporto provvede a crearlo estraendolo dal campo "From" originale.
Per l'invio delle ricevute, il sistema usa come destinatario il mittente del messaggio originale. Questo è ricavato dal campo "Reply-To" o, in sua assenza, dal campo "From" dell'intestazione originale del messaggio.
Tutti i messaggi generati dal sistema di posta certificata sono identificabili per la presenza di un header specifico. Questo header è utile per impedire loop di messaggi nel caso di scambio tra sistemi che prevedono l'invio di ricevute/messaggi di trasporto. È infatti possibile che un messaggio inviato da una casella di posta certificata e destinato ad un'altra casella anch'essa appartenente al servizio di posta certificata inneschi uno scambio improprio di messaggi. La ricezione di una ricevuta potrebbe infatti far scattare nel sistema la generazione di un'ulteriore ricevuta. Per ovviare a tale problema il sistema deve controllare l'eventuale presenza dell'header identificativo per verificare la natura del messaggio.

**Ai fini della determinazione dei dati di certificazione fanno fede, per il sistema, gli elementi utilizzati per l'effettivo instradamento del messaggio verso i destinatari. Nelle fasi di colloquio mediante protocollo SMTP (ad esempio presso i punti di accesso e di ricezione) i dati di "reverse path" e "forward path" (comandi "MAIL FROM" e "RCPT TO") sono quindi considerati come dati di certificazione rispettivamente del mittente e dei destinatari. I dati di indirizzamento presenti nel corpo del messaggio (campi "To" e "Cc") sono usati esclusivamente per discriminare tra destinatari primari del messaggio e riceventi in copia, qualora necessario.**

## Log

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema deve mantenere traccia delle operazioni svolte. Tutte le attività sono memorizzate su un registro riportante i dati significativi dell'operazione:

- il codice identificativo univoco del messaggio originale (Message-ID)
- la data e l'ora dell'evento
- il mittente del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
- il codice identificativo dei messaggi generati (ricevute, errori, ecc.)
- il server mittente

il server destinatario

Gli effettivi dati registrati sui singoli log dipendono dalla tipologia dell'operazione tracciata (ricezione di un messaggio, generazione ricevute, ecc.).

## Punto di accesso

Al momento dell'invio di un messaggio di posta certificata il punto di accesso deve accertare l'identità di chi effettua il collegamento. La modalità per l'accertamento dell'identità di un utente abilitato all'utilizzo del servizio deve poter prevedere, ove disponibili, l'utilizzo della carta d'identità elettronica o della carta nazionale dei servizi. Tale verifica è necessaria esclusivamente per garantire che il messaggio sia inviato da un utente del servizio di posta certificata. Il punto di accesso non verifica che il mittente specificato nel messaggio sia congruente con i dati di identificazione dell'utente.
Alla ricezione di un messaggio originale, il punto di accesso:
effettua dei controlli formali sul messaggio in ingresso;
genera una ricevuta di accettazione;
imbusta il messaggio originale in un messaggio di trasporto.

La ricevuta di accettazione indica al mittente che il suo messaggio è stato accettato dal sistema e certifica la data e l'ora dell'evento. All'interno della ricevuta è presente un testo leggibile dall'utente, un allegato XML con i dati di certificazione in formato elaborabile ed eventuali altri allegati per funzionalità aggiuntive offerte dal gestore.
Il punto di accesso, utilizzando i dati dell'indice dei gestori di posta certificata (cfr. 0), effettua un controllo per ogni destinatario del messaggio originale per verificare se appartengono all'infrastruttura di posta certificata o sono utenti esterni (es. posta Internet). La ricevuta di accettazione (ed i relativi dati di certificazione) riporta quindi la tipologia dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi (utenti di posta certificata, utenti esterni).
Il meccanismo di sicurezza per il colloquio tra i server partecipanti all'infrastruttura di posta certificata è realizzato mediante imbustamento e firma dei messaggi in uscita dal punto di accesso e la loro verifica in ingresso al punto di ricezione. Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di un messaggio di trasporto. Il messaggio di trasporto firmato permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario. La firma apposta sul messaggio dal sistema mittente è verificata all'arrivo sul server di destinazione.
Il dominio ricevente dovrà effettuare esclusivamente dei controlli formali sul messaggio ricevuto inoltrando il messaggio di trasporto immodificato al destinatario. Rispetto ad una soluzione che prevede la ritrasformazione del messaggio di trasporto nel messaggio originario, si ottiene la visibilità dei dati di certificazione inseriti dal messaggio (testo, XML, ulteriori allegati) permettendone così la verifica da parte del destinatario.
La sicurezza tra mittente e destinatario è completata mediante un meccanismo di protezione per le connessioni esterne all'architettura di posta certificata (tra utente e punto di accesso e tra punto di consegna ed utente) attuato tramite l'impiego di canali sicuri. L'integrità e la confidenzialità delle connessioni tra il gestore di posta certificata e l'utente devono essere realizzate mediante l'uso di protocolli sicuri (es. basati su TLS come imaps, pop3s) o che prevedano l'attivazione di un canale sicuro durante il colloquio (es. SMTP STARTTLS, POP3 STLS).
Deve essere garantita l'univocità dell'identificativo dei messaggi originali accettati nel complesso dell'infrastruttura di posta certificata per consentire una corretta tracciatura dei messaggi e delle relative ricevute.
Il formato di tale identificativo è del tipo:

```
[stringa alfanumerica]@[dominio_di_posta_gestore]
```

oppure:

```
[stringa alfanumerica]@[FQDN_server_di_posta]
```

Il messaggio originale ed il corrispondente messaggio di trasporto dovranno quindi contenere il seguente campo di header:

```
Message-ID: <[identificativo messaggio]>
```

**Qualora il client di posta elettronica che colloquia con il punto di accesso avesse già inserito un Message ID all'interno del messaggio originale da inviare, questo dovrà essere sostituito con l'identificativo sopra descritto.**

### Controlli formali sui messaggi in ingresso

Al momento dell'accettazione del messaggio il punto di accesso deve garantirne la correttezza formale verificando che:

nel corpo del messaggio esista un campo "From" riportante un indirizzo email conforme alle specifiche RFC 2822 §3.4.1;

nel corpo del messaggio esista un campo "To" riportante uno o più indirizzi email conformi alle specifiche RFC 2822 §3.4.1;

l'indirizzo del mittente del messaggio specificato nei dati di instradamento (reverse path) coincida con quanto specificato nel campo "From" del messaggio;

gli indirizzi dei destinatari del messaggio specificati nei dati di instradamento (forward path) coincidano con quelli presenti nei campi "To" o "Cc" del messaggio.

Qualora il messaggio non fosse formalmente valido, il punto di accesso dovrà non accettare il messaggio all'interno del sistema di posta certificata non emettendo, quindi, la relativa ricevuta di accettazione.

### Ricevuta di accettazione

La ricevuta di accettazione è costituita da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di accettazione, dati del mittente e del destinatario ed oggetto.
Negli header della ricevuta di accettazione sono inseriti i seguenti campi:

```
X-Ricevuta: accettazione
Date: [effettiva data di accettazione]
Subject: ACCETTAZIONE: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente messaggio originale]
```

Il primo campo identifica il messaggio come ricevuta di accettazione. Il campo "Subject" indica al destinatario che il messaggio è la ricevuta di una sua comunicazione. È composto dalla stringa "ACCETTAZIONE:" seguita dal subject del messaggio originale a cui la ricevuta fa riferimento.
Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello riportante i seguenti dati:

```
Ricevuta di accettazione
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente]"
ed indirizzato a:
[destinatario1] (["posta certificata" | "posta ordinaria"])
[destinatario2] (["posta certificata" | "posta ordinaria"])
.
.
.
[destinatarion] (["posta certificata" | "posta ordinaria"])
è stato accettato dal sistema.
Identificativo messaggio: [identificativo]
```

**Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.**

### Messaggio di trasporto

Il messaggio di trasporto consiste in un messaggio generato dal punto di accesso e che contiene il messaggio originale ed i dati di certificazione.
Il messaggio di trasporto eredita dal messaggio originale i seguenti header che dovranno quindi essere riportati immodificati:

Received
To
Cc
Return-Path

Message-ID (così come descritto al punto 0)
X-TipoRicevuta

Dovranno invece essere modificati, od inseriti se necessario, gli header sotto elencati:

```
X-Trasporto: posta-certificata
Date: [effettiva data di accettazione]
Subject: POSTA CERTIFICATA: [subject originale]
From: "[mittente originale]" <posta-certificata@[dominio_di_posta]>
Reply-To: [mittente originale (inserito solo se assente)]
```

Il corpo del messaggio di trasporto è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio di posta certificata secondo un modello che riporti i seguenti dati di certificazione:

```
Messaggio di posta certificata
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" è stato inviato da "[mittente]"
indirizzato a:
[destinatario1]
[destinatario2]
.
.
.
[destinatarion]
Il messaggio originale è incluso in allegato.
Identificativo messaggio: [identificativo]
```

All'interno del messaggio di trasporto è inserito in allegato l'intero messaggio originale immodificato in formato conforme alla RFC 2822 (tranne per quanto detto a proposito del Message ID) completo di header, corpo ed eventuali allegati. Nello stesso messaggio di trasporto è inoltre incluso un allegato XML che specifica in formato elaborabile i dati di certificazione già riportati nel testo. Al messaggio di trasporto possono inoltre essere allegati ulteriori elementi opzionali per specifiche funzionalità fornite dal gestore di posta certificata.

**Anche se il campo "From" del messaggio di trasporto è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento del messaggio di trasporto (forward path e reverse path) rimangono immutati rispetto agli stessi dati del messaggio originale. In questo modo è garantito sia l'inoltro del messaggio verso i destinatari originari sia il ritorno di eventuali notifiche di errore sul protocollo SMTP (come da RFC 2821 e RFC 1891) al mittente del messaggio originale.**

### Punto di ricezione

Il punto di ricezione permette lo scambio di messaggi di posta certificata tra diversi gestori di posta certificata. È inoltre il punto attraverso il quale, messaggi di posta elettronica ordinaria possono essere inseriti nel circuito della posta certificata (cfr. schemi in appendice).
Lo scambio di messaggi tra diversi gestori avviene tramite una transazione basata sul protocollo SMTP come definita dalla RFC 2821. I messaggi sono trasferiti tra gestori usando una codifica a 7 bit sia per gli header sia per il corpo del messaggio e gli eventuali allegati. Eventuali errori derivanti dal colloquio SMTP (es. destinatari non validi, server non disponibile, ecc.) sono gestiti mediante i meccanismi standard di notifica degli errori propri del protocollo SMTP.
Il punto di ricezione, a fronte dell'arrivo di un messaggio, effettua la seguente serie di controlli ed operazioni:

- verifica la correttezza/natura del messaggio in ingresso;
- se il messaggio in ingresso è un messaggio di trasporto corretto:
  - emette una ricevuta di presa in carico verso il gestore mittente (cfr. 0);
  - inoltra il messaggio di trasporto verso il punto di consegna (cfr. 0);
- se il messaggio in ingresso è un messaggio di trasporto errato/non è un messaggio di trasporto:
  - imbusta il messaggio in arrivo in un messaggio di anomalia di trasporto (cfr. 0);
  - inoltra il messaggio di anomalia di trasporto verso il punto di consegna.

**La ricevuta di presa in carico è emessa dal gestore ricevente il messaggio nei confronti del gestore mittente. Il suo fine è quello di consentire il tracciamento del messaggio nel passaggio tra un gestore ed un altro.**

### Verifiche sui messaggi in ingresso

Al ricevimento di un messaggio presso il punto di ricezione, il sistema effettua una serie di controlli per verificare che il messaggio di trasporto sia corretto/integro:

Controllo dell'esistenza della firma

Il sistema verifica la presenza della struttura S/MIME di firma all'interno del messaggio in ingresso.

Controllo che la firma sia stata emessa da un gestore di posta certificata

Il punto di ricezione estrae il certificato usato per la firma del messaggio in ingresso e ne verifica la presenza all'interno dell'indice dei gestori di posta certificata.

Controllo della validità della firma

È verificata la correttezza della firma S/MIME del messaggio effettuando il ricalcolo degli algoritmi di firma.

Se tutti i controlli hanno esito positivo, il sistema stabilisce che il messaggio in ingresso è un messaggio di trasporto corretto altrimenti lo considera come errato o di posta ordinaria.

### Ricevuta di presa in carico

Allo scambio di messaggi di posta certificata corretti tra differenti gestori di posta certificata, il gestore ricevente emette una ricevuta di presa in carico nei confronti del gestore mittente. Le ricevute di presa in carico emesse sono relative ai destinatari ai quali è indirizzato il messaggio in ingresso, così come specificato nei dati di instradamento (forward path e reverse path) della transazione SMTP. All'interno dei dati di certificazione della singola ricevuta di presa in carico sono elencati i destinatari a cui la stessa fa riferimento. In generale, a fronte di un messaggio di trasporto ogni gestore destinatario dovrà emettere una o più ricevute di presa in carico per i destinatari di propria competenza. L'insieme di tali ricevute coprirà, in assenza di errori di trasporto, il complessivo dei destinatari del messaggio.
Gli header di una ricevuta di presa in carico contengono i seguenti campi:

```
X-Ricevuta: presa-in-carico
Date: [data di presa in carico]
Subject: PRESA IN CARICO: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [ricevute gestore mittente]
```

L'indirizzo per l'invio delle ricevute al gestore mittente è ricavato dall'indice dei gestori di posta certificata durante l'interrogazione necessaria per il controllo del soggetto che ha emesso la firma nella verifica del messaggio in ingresso.
Il corpo del messaggio di una ricevuta di presa in carico è composto secondo un modello riportante i seguenti dati:

```
Ricevuta di presa in carico
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente]"
ed indirizzato a:
[destinatario1]
[destinatario2]
.
.
.
[destinatarion]
è stato accettato dal sistema.
Identificativo messaggio: [identificativo]
```

**Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.**

### Messaggio di anomalia di trasporto

Qualora uno dei test evidenzi un errore nel messaggio in arrivo, il sistema lo inserisce in un messaggio di anomalia di trasporto. Prima della consegna, il messaggio pervenuto al punto di ricezione completo di header,

testo ed allegati è inserito in formato conforme alla RFC 2822 come allegato all'interno di un nuovo messaggio che eredita dal messaggio in arrivo i seguenti header che dovranno quindi essere riportati immodificati:

Received
To
Cc
Return-Path
Message-ID

Dovranno invece essere modificati, od inseriti se necessario, gli header sotto elencati:

```
X-Trasporto: errore
Date: [data di arrivo del messaggio]
Subject: ANOMALIA MESSAGGIO: [subject originale]
From: "[mittente originale]" <posta-certificata@[dominio_di_posta]>
Reply-To: [mittente originale (inserito solo se assente)]
```

Il corpo del messaggio di anomalia di trasporto è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio secondo un modello che riporti i seguenti dati:

```
Anomalia nel messaggio
Il giorno [data] alle ore [ora] ([zona]) è stato ricevuto
il messaggio "[subject]" proveniente da "[mittente]"
ed indirizzato a:
[destinatario1]
[destinatario2]
.
.
.
[destinatarion]
Tali dati non sono stati certificati per il seguente errore:
[descrizione sintetica errore riscontrato]
Il messaggio originale è incluso in allegato.
```

Nel messaggio di anomalia di trasporto non sono inseriti allegati oltre al messaggio pervenuto al punto di ricezione (es. dati di certificazione) data l'incertezza sull'effettiva provenienza/correttezza del messaggio.
Anche se il campo "From" del messaggio di anomalia di trasporto è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento del messaggio di trasporto (forward path e reverse path) rimangono immutati rispetto agli stessi dati del messaggio originale. In questo modo è garantito sia l'inoltro del messaggio verso i destinatari originari sia il ritorno di eventuali notifiche di errore sul protocollo SMTP (come da RFC 2821 e RFC 1891) al mittente del messaggio.

## Punto di consegna

### Verifiche sui messaggi in ingresso

All'arrivo del messaggio presso il punto di consegna, il sistema ne verifica la tipologia e stabilisce se deve inviare una ricevuta al mittente. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione di un messaggio di trasporto valido, identificabile dalla presenza dell'header:

```
X-Trasporto: posta-certificata
```

In tutti gli altri casi (es. messaggi di anomalia di trasporto), la ricevuta di avvenuta consegna non è emessa. In ogni caso, il messaggio ricevuto dal punto di consegna deve essere consegnato immodificato alla casella di posta del destinatario.
La ricevuta di avvenuta consegna indica al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato e certifica la data e l'ora dell'evento tramite un testo leggibile dall'utente ed un allegato XML con i dati di certificazione in formato elaborabile oltre ad eventuali allegati per funzionalità aggiuntive offerte dal gestore.
Se il messaggio pervenuto al punto di consegna non fosse recapitabile alla casella di destinazione, il punto di consegna emette una ricevuta di errore di consegna (cfr. 0). La ricevuta di errore di consegna è generata, a fronte

di un errore, esclusivamente nei casi previsti per la ricevuta di avvenuta consegna (arrivo di un messaggio di trasporto corretto).

### Ricevuta di avvenuta consegna

Le ricevute di avvenuta consegna sono costituite da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di avvenuta consegna, dati del mittente e del destinatario ed oggetto.
Negli header delle ricevute di avvenuta consegna sono inseriti i seguenti campi:

```
X-Ricevuta: avvenuta-consegna
Date: [data di consegna]
Subject: CONSEGNA: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente messaggio originale]
```

Il primo campo identifica il messaggio come ricevuta di avvenuta consegna. Il campo "Subject" indica al destinatario che il messaggio è la ricevuta di una sua comunicazione. È composto dalla stringa "CONSEGNA:" seguita dal subject del messaggio originale a cui la ricevuta fa riferimento.
Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati di certificazione:

```
Ricevuta di avvenuta consegna
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente]"
ed indirizzato a "[destinatario]"
è stato consegnato nella casella di destinazione.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.
Nel rilascio delle ricevute di avvenuta consegna, il sistema distingue tra i messaggi consegnati ai destinatari primari ed i riceventi in copia. Tale verifica è effettuata mediante l'analisi dei campi "To" (destinatari primari) e "Cc" (riceventi in copia) del messaggio rispetto al destinatario oggetto della consegna. Esclusivamente per le consegne relative ai destinatari primari, all'interno della ricevuta di avvenuta consegna, oltre agli allegati descritti, è inserito il messaggio originale completo (header, testo ed eventuali allegati). Qualora il sistema non potesse determinare con certezza la natura del destinatario (primario od in copia) per problemi di ambiguità dei campi "To" e "Cc", la consegna dovrà essere considerata come indirizzata ad un destinatario primario ed includere il messaggio originale completo.

### Ricevuta breve di avvenuta consegna

Se all'interno del messaggio di trasporto è presente l'intestazione:

```
X-TipoRicevuta: breve
```

il punto di consegna emette, per i destinatari primari, una ricevuta breve di avvenuta consegna. L'assenza di tale intestazione o un suo diverso valore comportano l'elaborazione della ricevuta di avvenuta consegna secondo le modalità già descritte al punto precedente. Il valore dell'intestazione nel messaggio di trasporto deriva dal messaggio originale (cfr. punto precedente) permettendo così al mittente di determinare il formato delle ricevute di avvenuta consegna relative ai destinatari primari del messaggio originale. Per i destinatari riceventi in copia, le ricevute di avvenuta consegna seguono quanto descritto al punto precedente.
Alla ricevuta breve di avvenuta consegna è allegato, invece del messaggio originale, un messaggio avente la stessa struttura MIME ma i cui allegati sono sostituiti da altrettanti file di testo contenenti gli hash del file al quale si vanno a sostituire. L'algoritmo utilizzato per il calcolo dell'hash è il Secure Hash Algorithm 1 (SHA1) così come descritto dalla RFC 3174 calcolato sull'intero contenuto dell'allegato. Per consentire di distinguere i file contenenti gli hash dai file a cui fanno riferimento, il suffisso "`.hash`" è aggiunto al termine del nome originale del file. L'hash è scritto all'interno del file con rappresentazione esadecimale come un'unica sequenza di 40 caratteri. Il MIME type di questi allegati è impostato a "`text/plain`" per evidenziare la loro natura testuale.

### Ricevuta di errore di consegna

Nel caso si verifichi un errore nella fase di consegna del messaggio, il sistema genera una ricevuta di errore di consegna da restituire al mittente con l'indicazione dell'errore riscontrato.
Per una ricevuta di errore di consegna gli header contengono i seguenti campi:

```
X-Ricevuta: errore-consegna
Date: [data di emissione ricevuta]
Subject: ERRORE: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente messaggio originale]
```

**Il corpo del messaggio di una ricevuta di errore di consegna è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:**

```
Errore di consegna del messaggio
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" proveniente da "[mittente]"
e destinato all'utente "[destinatario]"
è stato rilevato un errore [errore sintetico].
Il messaggio è stato rifiutato dal sistema.
Identificativo messaggio: [identificativo]
```

**Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.**

## Formati

### Riferimento temporale

**Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna è necessario disporre di un accurato riferimento temporale. Tutti gli eventi (generazione di ricevute, messaggi di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso, ricezione e consegna devono impiegare un unico valore temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, ricevute, messaggi, ecc. generati dal server. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca uno scarto non superiore ad 1 secondo rispetto al Tempo Universale Coordinato (UTC).**

### Formato data/ora utente

Le indicazioni temporali fornite dal servizio in formato leggibile dall'utente (testo delle ricevute, messaggi di trasporto, ecc.) sono fornite con riferimento all'ora legale vigente al momento indicato per l'operazione. Per la data il formato impiegato è "`gg/mm/aaaa`" mentre per l'indicazione oraria si utilizza "`hh:mm:ss`", dove *hh* è in formato 24 ore. Al dato temporale è fatta seguire tra parentesi la "zona" ossia la differenza (in ore e minuti) tra l'ora legale locale ed UTC. La rappresentazione di tale valore è in formato "`[+|-]hhmm`", dove il primo carattere indica una differenza positiva o negativa.

### Specifiche degli allegati

**Di seguito sono riportati i dati caratteristici delle varie componenti di messaggi e ricevute generati dal sistema di posta certificata. Nel caso in cui una delle parti del messaggio contenesse caratteri con valori al di fuori dell'intervallo 0÷127 (7-bit ASCII) la parte dovrà essere adeguatamente codificata in maniera tale da garantire che il messaggio finale sia compatibile con il trasporto a 7 bit previsto (es. quoted-printable, base64).**

### Corpo del messaggio

Set di caratteri: `ISO-8859-1 (Latin-1)`
MIME type: `text/plain` oppure `multipart/alternative`

Il MIME type `multipart/alternative` può essere utilizzato per aggiungere una versione in formato HTML del corpo dei messaggi generati dal sistema. In questo caso dovranno essere presenti due sotto-parti MIME: una di tipo `text/plain` ed un'altra `text/html`. La parte in formato HTML deve rispettare i seguenti vincoli:

- deve contenere le stesse informazioni riportate nella parte di testo;
- non deve contenere riferimenti ad elementi (es. immagini, suoni, font, style sheet) né interni al messaggio (parti MIME aggiuntive) né esterni (es. ospitati su server del gestore);
- non deve avere contenuto attivo (es. Javascript, VBscript, Plug-in, ActiveX).

### Messaggio originale

MIME type: `message/rfc822`
Nome allegato: `postacert.eml`

### Dati di certificazione

Set di caratteri: `UTF-8`
MIME type: `application/xml`
Nome allegato: `daticert.xml`

### Dati di certificazione

Di seguito viene proposto il DTD relativo al file XML che conterrà i dati di certificazione da allegare nelle ricevute.

```
<?xml version="1.0" encoding="UTF-8"?>

<!--Usare l'elemento "postacert" come radice-->
<!--"tipo" indica la tipologia del messaggio di posta certificata-->
<!--L'attributo "errore" può avere i seguenti valori-->
<!--"nessuno" = nessun errore-->
<!--"no-dest" (con tipo="errore-consegna") = destinatario errato-->
<!--"no-dominio" (con tipo="errore-consegna") = dominio errato-->
<!--"altro" = errore generico-->
<!ELEMENT postacert (intestazione, dati)>
<!ATTLIST postacert
      tipo (accettazione |
            presa-in-carico |
            avvenuta-consegna |
            posta-certificata |
            errore-consegna) #REQUIRED
      errore (nessuno |
              no-dest |
              no-dominio |
              altro) "nessuno">

<!--Intestazione del messaggio originale-->
<!ELEMENT intestazione (mittente,
                        destinatari+,
                        risposte,
                        oggetto?)>

<!--Mittente (campo "From") del messaggio originale-->
<!ELEMENT mittente (#PCDATA)>

<!--Elenco completo dei destinatari (campi "To" e "Cc")-->
<!--del messaggio originale-->
<!--"tipo" indica la tipologia del destinatario-->
<!ELEMENT destinatari (#PCDATA)>
```

```
<!ATTLIST destinatari
      tipo (certificato | esterno) "certificato">

<!--Valore del campo "Reply-To" del messaggio originale-->
<!ELEMENT risposte (#PCDATA)>

<!--Valore del campo "Subject" del messaggio originale-->
<!ELEMENT oggetto (#PCDATA)>

<!--Dati del messaggio di posta certificata-->
<!ELEMENT dati (gestore-emittente,
                data,
                identificativo,
                consegna?,
                ricezione*,
                errore-esteso?)>

<!--Stringa descrittiva del gestore che certifica i dati-->
<!ELEMENT gestore-emittente (#PCDATA)>

<!--Data/ora di elaborazione del messaggio-->
<!--"zona" e' la differenza tra ora legale locale ed UTC in-->
<!--formato "[+|-]hhmm"-->
<!ELEMENT data (giorno, ora)>
<!ATTLIST data
      zona CDATA #REQUIRED>

<!--Giorno in formato "gg/mm/aaaa"-->
<!ELEMENT giorno (#PCDATA)>

<!--Ora locale in formato "hh:mm:ss"-->
<!ELEMENT ora (#PCDATA)>

<!--Identificativo univoco del messaggio originale-->
<!ELEMENT identificativo (#PCDATA)>

<!--Per le ricevute di consegna e di errore di consegna-->
<!--Destinatario a cui e' stata effettuata/tentata la consegna-->
<!ELEMENT consegna (#PCDATA)>

<!--Per le ricevute di presa in carico-->
<!--Destinatari per i quali e' relativa la ricevuta-->
<!ELEMENT ricezione (#PCDATA)>

<!--In caso di errore-->
<!--Descrizione sintetica errore-->
<!ELEMENT errore-esteso (#PCDATA)>
```

## Schema indice dei gestori di posta certificata

L'indice dei gestori di posta certificata è realizzato mediante un server LDAP centralizzato che contiene i dati dei gestori e dei relativi domini di posta certificata. Il contenuto di tale indice è interrogabile sia tramite LDAP che via HTTP su protocollo TLS per garantirne l'autenticità e l'integrità. La "base root" dell'indice è "`o=postacert`" ed i "DistinguishedName" dei singoli record sono del tipo "`providerName=<nome>,o=postacert`". La ricerca all'interno dell'indice avviene principalmente usando gli attributi "`providerCertificateSubject`" o "`managedDomains`". L'attributo "`LDIFLocationURL`" deve puntare ad un oggetto HTTP/HTTPS, messo a disposizione dal gestore, che contiene un file in formato LDIF secondo RFC 2849. Tale file LDIF è scaricato con cadenza regolare dal sistema

LDAP centralizzato ed applicato sul record relativo al gestore. Il file LDIF che comprende i dati di tutti i gestori di posta certificata è disponibile, come oggetto HTTPS, alla URL puntata dall'attributo "LDIFLocationURL" del record "dn: o=postacert". Mediante tale LDIF, i singoli gestori dovranno replicare periodicamente il contenuto dell'indice localmente, al fine di migliorare i tempi di risposta del sistema evitando di effettuare richieste LDAP per ogni fase di elaborazione del messaggio.

**Di seguito sono riportati gli attributi definiti per lo schema dell'indice dei gestori di posta certificata:**

| Nome attributo | Sintassi | Descrizione |
|---|---|---|
| providerCertificateSubject | DN | Riporta il "subject DN" contenuto nel certificato usato dal gestore per la firma delle ricevute e dei messaggi di trasporto |
| providerCertificate | Certificate<br>Binary transfer | Certificato/i usato/i dal gestore per la firma delle ricevute e dei messaggi di trasporto |
| providerName | Directory string<br>Single value | Nome del gestore di posta certificata |
| mailReceipt | IA5 string<br>Single value | Indirizzo di posta elettronica a cui inviare le ricevute di presa in carico |
| managedDomains | IA5 string | Domini di posta certificata amministrati dal gestore |
| LDIFLocationURL | Directory string<br>Single value | URL HTTP dove è mantenuta la definizione in formato LDIF del record relativo al gestore (dell'intero indice per il record "dn: o=postacert") |

**Quello che segue è lo schema LDAP per l'indice dei gestori di posta certificata secondo la sintassi descritta nella RFC 2252:**

```
attributetype ( 16572.2.2.1
        NAME 'providerCertificateSubject'
        DESC 'Subject DN del certificato X.509 del gestore'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

attributetype ( 16572.2.2.2
        NAME 'providerCertificate'
        DESC 'Certificato X.509 in formato binario ASN.1 DER'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )

attributetype ( 16572.2.2.3
        NAME 'providerName'
        DESC 'Nome del gestore di posta certificata'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
        SINGLE-VALUE )

attributetype ( 16572.2.2.4
        NAME 'mailReceipt'
        DESC 'E-mail a cui inviare le ricevute di presa in carico'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256}
        SINGLE-VALUE )

attributetype ( 16572.2.2.5
        NAME 'managedDomains'
        DESC 'Domini gestiti dal gestore di posta certificata'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

attributetype ( 16572.2.2.6
```

```
        NAME 'LDIFLocationURL'
        DESC 'URL (HTTP) del file LDIF che definisce la entry'
        EQUALITY caseExactMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

objectclass ( 16572.2.1.1
        NAME 'LDIFLocationURLObject'
        DESC 'Classe per inserimento di un attributo LDIFLocationURL'
        MAY ( LDIFLocationURL )
        SUP top AUXILIARY )

objectclass ( 16572.2.1.2
        NAME 'provider'
        DESC 'Gestore di posta certificata'
        SUP top
        MUST    ( providerCertificateSubject $
                  providerCertificate $
                  providerName $
                  mailReceipt $
                  managedDomains $
                  LDIFLocationURL )
        MAY     ( description ) )
```

Il seguente file LDIF rappresenta un esempio di indice dei gestori della posta certificata contenente una “base root” e due gestori fittizi. I certificati inseriti sono due certificati “self-signed” riportati a titolo di esempio:

```
dn: o=postacert
objectclass: top
objectclass: organization
objectClass: LDIFLocationURLObject
o: postacert
LDIFLocationURL: https://postacert.ct.rupa.it/postacert.ldif
description: Base root per l’indice dei gestori di posta certificata

dn: providerName=Anonima Posta Certificata S.p.A.,o=postacert
objectclass: top
objectclass: provider
providerName: Anonima Posta Certificata S.p.A.
providerCertificateSubject: C=IT, O=Anonima Posta Certificata S.p.A.,
 Email=posta-certificata@anpocert.it
providerCertificate;binary:: MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBmMQswCQYDVQQGEwJJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZp
 Y2F0YSBTLnAuQS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG
 9jZXJ0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkGA1UE
 BhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdGEgUy5wLkEuMS
 wwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBhbnBvY2VydC5pdDCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qKKdxV9LzDMPqwnEy0P8H/KwbI0Szs
 8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC2uL09HDyx8agjgZWdhypnehguiSK3busha15
 RSpMGhiqxmz2b0HhOG73GfalZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxz
 y34XcCAwEAAaOBwzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAG
 A1UdIwSBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYTAk
 lUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC5BLjEsMCoG
 CSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2NlcnQuaXSCAQAwDAYDVR
 0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58BZ+q1qSKpuffzTBpMtbeFkDIxMq
 Ma+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqAXxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIw
 bOunhrvsxh3vsG5CgN76JzZ95Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2Vl
 xlQP7McSUw==
mailReceipt: ricevute@anpocert.it
LDIFLocationURL: http://www.anpocert.it/LDIF/anpocert.ldif
```

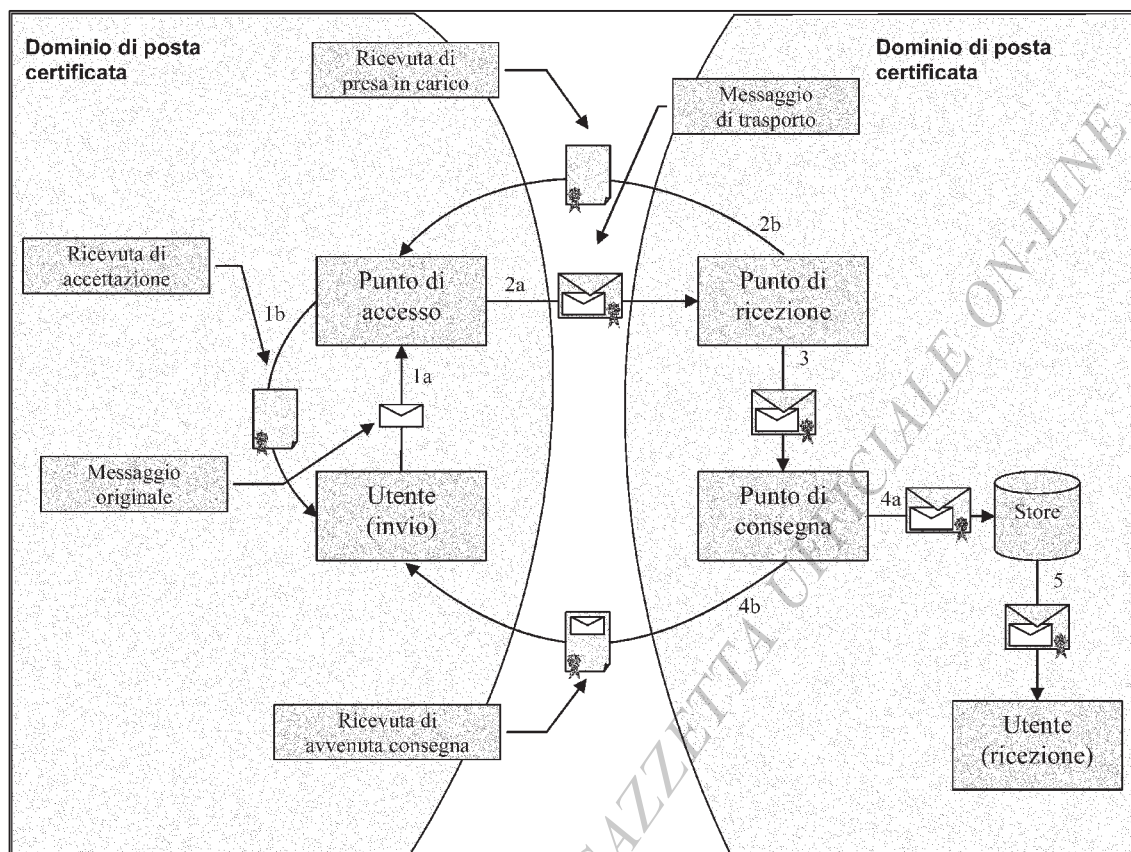
```
managedDomains: posta.anpocert.it
managedDomains: cert.azienda.it
managedDomains: costmec.it
description: Servizi di posta certificata per aziende

dn: providerName=Servizi Postali S.r.l.,o=postacert
objectclass: top
objectclass: provider
providerName: Servizi Postali S.r.l.
providerCertificateSubject: C=IT, O=Servizi Postali S.r.l.,
OU=D.C.C.,
 Email=posta-certificata@serpostal.it
providerCertificate;binary:: MIIDHjCCAoegAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXQwHhcNMDIxMjA5MTczMjE2WhcNMDMxMjA5MTczMjE2WjBu
 MQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5sLjEPMA
 0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2F0YUBz
 ZXJwb3N0YWwuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKoc7n6zA+sO8N
 ATMcfJ+U2aoDEsrj/cObG3QAN6Sr+lygWxYXLBZNfSDWqL1K4edLr4gCZIDFsq0PIE
 aYZhYRGjhbcuJ9H/ZdtWdXxcwEWN4mwFzlsASogsh5JeqS8db3A1JWkvhO9EUfaCYk
 8YMAkXYdCtLD9s9tCYZeTE2ut9AgMBAAGjgcswgcgwHQYDVR0OBBYEFHPw7VJIoIM3
 VYhuHaeAwpPF5leMMIGYBgNVHSMEgZAwgY2AFHPw7VJIoIM3VYhuHaeAwpPF5leMoX
 KkcDBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOB
 gQApqeXvmOyEjwhMrXezPAXELMZwv4qqr5ri4XuxTq6sS9jRsEbZrS+NmbcJ7S7eFw
 NQMNxYFVJqdWoLh8qExsTLXnsKycPSnHbCfuphrKvXjQvR2da75U4zGSkroiyvJ2s9
 TtiCcT3lQtIjmvrFbaSBiyzj+za7foFUCQmxCLtDaA==
mailReceipt: presaincarico@serpostal.it
LDIFLocationURL: http://servizi.serpostal.it/ldif.txt
managedDomains: servizi-postali.it
managedDomains: postaricevuta.it
description: Servizi di posta certificata per il pubblico
```



# APPENDICE

## Schema logico di funzionamento

**Nel seguito viene proposta una rappresentazione grafica che schematizza gli elementi caratteristici di un dominio di posta certificata e le sue interazioni con un altro dominio di posta certificata.**

**04A010341**

GIANFRANCO TATOZZI, *direttore* FRANCESCO NOCITA, *redattore*

(G403130/1) Roma, 2004 - Istituto Poligrafico e Zecca dello Stato S.p.A. - S.

# GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

## CANONI DI ABBONAMENTO ANNO 2005 (salvo conguaglio) (*)

Ministero dell'Economia e delle Finanze - *Decreto 24 dicembre 2003* (G.U. *n. 36 del 13 febbraio 2004)*

**GAZZETTA UFFICIALE - PARTE I** (legislativa)

| | | CANONE DI ABBONAMENTO | | |
|---|---|---|---|---|
| **Tipo A** | Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari: | | | |
| | *(di cui spese di spedizione € 219,04)* | - annuale | € | **400,00** |
| | *(di cui spese di spedizione € 109,52)* | - semestrale | € | **220,00** |
| **Tipo A1** | Abbonamento ai fascicoli della serie generale, inclusi i soli supplementi ordinari contenenti i provvedimenti legislativi: | | | |
| | *(di cui spese di spedizione € 108,57)* | - annuale | € | **285,00** |
| | *(di cui spese di spedizione € 54,28)* | - semestrale | € | **155,00** |
| **Tipo B** | Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte Costituzionale: | | | |
| | *(di cui spese di spedizione € 19,29)* | - annuale | € | **68,00** |
| | *(di cui spese di spedizione € 9,64)* | - semestrale | € | **43,00** |
| **Tipo C** | Abbonamento ai fascicoli della serie speciale destinata agli atti della CE: | | | |
| | *(di cui spese di spedizione € 41,27)* | - annuale | € | **168,00** |
| | *(di cui spese di spedizione € 20,63)* | - semestrale | € | **91,00** |
| **Tipo D** | Abbonamento ai fascicoli della serie destinata alle leggi e regolamenti regionali: | | | |
| | *(di cui spese di spedizione € 15,31)* | - annuale | € | **65,00** |
| | *(di cui spese di spedizione € 7,65)* | - semestrale | € | **40,00** |
| **Tipo E** | Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni: | | | |
| | *(di cui spese di spedizione € 50,02)* | - annuale | € | **167,00** |
| | *(di cui spese di spedizione € 25,01)* | - semestrale | € | **90,00** |
| **Tipo F** | Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari, ed ai fascicoli delle quattro serie speciali: | | | |
| | *(di cui spese di spedizione € 344,93)* | - annuale | € | **780,00** |
| | *(di cui spese di spedizione € 172,46)* | - semestrale | € | **412,00** |
| **Tipo F1** | Abbonamento ai fascicoli della serie generale inclusi i supplementi ordinari con i provvedimenti legislativi e ai fascicoli delle quattro serie speciali: | | | |
| | *(di cui spese di spedizione € 234,45)* | - annuale | € | **652,00** |
| | *(di cui spese di spedizione € 117,22)* | - semestrale | € | **342,00** |

**N.B.:** L'abbonamento alla GURI tipo A, A1, F, F1 comprende gli indici mensili
*Integrando con la somma di €* **80,00** *il versamento relativo al tipo di abbonamento alla* Gazzetta Ufficiale - *parte prima - prescelto, si riceverà anche l'Indice Repertorio Annuale Cronologico per materie anno 2005.*

**BOLLETTINO DELLE ESTRAZIONI**

Abbonamento annuo (incluse spese di spedizione) € **88,00**

**CONTO RIASSUNTIVO DEL TESORO**

Abbonamento annuo (incluse spese di spedizione) € **56,00**

**PREZZI DI VENDITA A FASCICOLI**
(Oltre le spese di spedizion e)

| Prezzi di vendita: | | |
|---|---|---|
| serie generale | € | 1,00 |
| serie speciali (escluso concorsi), ogni 16 pagine o frazione | € | 1,00 |
| fascicolo serie speciale, *concorsi,* prezzo unico | € | 1,50 |
| supplementi (ordinari e straordinari), ogni 16 pagine o frazione | € | 1,00 |
| fascicolo Bollettino Estrazioni, ogni 16 pagine o frazione | € | 1,00 |
| fascicolo Conto Riassuntivo del Tesoro, prezzo unico | € | 6,00 |

I.V.A. 4% a carico dell'Editore

**GAZZETTA UFFICIALE - PARTE II** (inserzioni)

| | | | |
|---|---|---|---|
| Abbonamento annuo *(di cui spese di spedizione € 120,00)* | | € | **320,00** |
| Abbonamento semestrale *(di cui spese di spedizione € 60,00)* | | € | **185,00** |
| Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione (oltre le spese di spedizione) | € 1,00 | | |

I.V.A. 20% inclusa

**RACCOLTA UFFICIALE DEGLI ATTI NORMATIVI**

| | | | |
|---|---|---|---|
| Abbonamento annuo | | € | **190,00** |
| Abbonamento annuo per regioni, province e comuni | | € | **180,00** |
| Volume separato (oltre le spese di spedizione) | € 18,00 | | |

I.V.A. 4% a carico dell'Editore

Per l'estero i prezzi di vendita, in abbonamento ed a fascicoli separati, anche per le annate arretrate, compresi i fascicoli dei supplementi ordinari e straordinari, devono intendersi raddoppiati. Per il territorio nazionale i prezzi di vendita dei fascicoli separati, compresi i supplementi ordinari e straordinari, relativi ad anni precedenti, devono intendersi raddoppiati. Per intere annate è raddoppiato il prezzo dell'abbonamento in corso. Le spese di spedizione relative alle richieste di invio per corrispondenza di singoli fascicoli, vengono stabilite, di volta in volta, in base alle copie richieste.

**N.B. - Gli abbonamenti annui decorrono dal 1° gennaio al 31 dicembre, i semestrali dal 1° gennaio al 30 giugno e dal 1° luglio al 31 dicembre.**

Restano confermati gli sconti in uso applicati ai soli costi di abbonamento

**ABBONAMENTI UFFICI STATALI**
Resta confermata la riduzione del 52% applicata sul solo costo di abbonamento

* tariffe postali di cui al Decreto 13 novembre 2002 (G.U. n. 289/2002) e D.P.C.M. 27 novembre 2002 n. 294 (G.U. 1/2003) per soggetti iscritti al R.O.C.